MYKOLO ROMERIO UNIVERSITETAS

LIETUVOS KIBERNETINIO SAUGUMO STRATEGIJOS MODELIS

Vilnius, 2017 m.

MYKOLO ROMERIO UNIVERSITETAS

LIETUVOS KIBERNETINIO SAUGUMO STRATEGIJOS MODELIS[1]

Autorių kolektyvas:
dr. Darius Štitilis
dr. Paulius Pakutinskas
dr. Marius Laurinaitis
Inga Malinauskaitė-van de Castel

Mykolo Romerio universitetas
Vilnius, 2017 m. kovo mėn.

1 Modelio kūrimą finansavo Lietuvos mokslo taryba. Projekto pavadinimas: „ES ir NATO valstybių kibernetinio saugumo strategijų normų analizė ir adaptavimas Lietuvos situacijai – Lietuvos kibernetinio saugumo strategijos modelis, Nr. MIP-099/2015.

MYKOLO ROMERIO UNIVERSITETAS

TURINYS

SĄVOKOS 4

SUTRUMPINIMAI 5

ĮVADAS 6

1. MODELIO METODOLOGIJA IR BENDRIEJI PASTEBĖJIMAI DĖL MODELIO BEI STRATEGIJOS 7

1.1. Lietuvos kibernetinio saugumo strategijos modelio metodologija 7
1.2. Bendrieji pastebėjimai dėl Lietuvos kibernetinio saugumo strategijos modelio bei strategijos 13

2. LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO SITUACIJOS APŽVALGA 15

2.1. Kibernetinio saugumo grėsmių ir geopolitinės situacijos Lietuvos Respublikoje apžvalga 15
2.2. Kibernetinio saugumo strategijų / programų Lietuvoje apžvalga 19
2.3. Teisinės aplinkos Lietuvoje apžvalga 23

3. PRINCIPAI 33

4. KIBERNETINIO SAUGUMO TIKSLAI, PAGRINDINĖS VEIKSMŲ SRITYS IR PRIORITETAI 38

4.1. Kibernetinio saugumo strategijos tikslai 39
4.2. Pagrindinės veiksmų sritys 40
4.3. Prioritetų turinys 43

5. KIBERNETINIO SAUGUMO VALDYMO SISTEMA 47

6. KIBERNETINIS SAUGUMAS NACIONALINĖJE SAUGUMO SISTEMOJE 50

6.1. Strategijos ryšys su teisės aktais 50
6.2. Saugumas bendrąja prasme 50
6.3. Kibernetinis saugumas 50

7. MODELIO NAUDOJIMO GAIRĖS IR TYRIMO RIBOTUMAI 52

7.1. Modelio naudojimo gairės 52
7.2. Tyrimo apribojimai 54

NAUDOTA LITERATŪRA 55

PRIEDAI 57

Priedas Nr. 1. Užsienio ekspertų aprašymas 57
Priedas Nr. 2. Klausimai užsienio ekspertams ir užsienio ekspertų atsakymai 59
Priedas Nr. 3. Lietuvos ekspertų aprašymas 78
Priedas Nr. 4. Klausimai Lietuvos ekspertams ir Lietuvos ekspertų apibendrinti atsakymai 79
Priedas Nr. 5. Publikuotų mokslo straipsnių kopijos 85

SĄVOKOS

Elektroninė erdvė – aplinka, kur galimas efektyvus veiksmas per atstumą pasinaudojant informacinėmis technologijomis.

Elektroninių ryšių tinklas – perdavimo sistemos ir atitinkamais atvejais komutavimo ar maršruto parinkimo įranga bei kiti ištekliai, kurie leidžia perduoti signalus laidais, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuoto (komutuojamas ir paketinis duomenų perdavimas, įskaitant internetą) ir judriojo ryšio antžeminius tinklus, elektros perdavimo kabelines sistemas, tokiu mastu, kokiu jos yra naudojamos signalams perduoti, radijo ir televizijos programų transliavimui naudojami tinklai ir kabelinės televizijos tinklai, neatsižvelgiant į perduodamos informacijos pobūdį;

Ypatingos svarbos informacinė infrastruktūra – elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams.

Pramoninių procesų valdymo sistema – iš informacinėmis ir ryšių technologijomis grindžiamos įrangos sudaryta sistema, skirta technologiniams procesams stebėti ar valdyti pramonės, energetikos, transporto, vandens tiekimo paslaugų ir kituose ūkinės veiklos sektoriuose.

Tinklų ir informacinių sistemų saugumas – tinklų ir informacinių sistemų pajėgumas tam tikru patikimumo lygiu išlikti atsparus bet kuriems veiksmams, keliantiems pavojų saugomų, perduodamų ar tvarkomų duomenų, arba atitinkamų teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui;

Rizika – pagrįstai nustatoma aplinkybė ar įvykis, galintis turėti neigiamą poveikį tinklų ir informacinių sistemų saugumui;

Incidentas – incidentas – įvykis, turintis faktinį neigiamą poveikį tinklų ir informacinių sistemų saugumui;

Incidentų valdymas – visos procedūros, padedančios nustatyti, ištirti bei suvaldyti incidentą ir į jį reaguoti.

SUTRUMPINIMAI

CERT-LT	Nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys
CSIRT	Reagavimo į kompiuterinius saugumo incidentus tarnybų tinklas
DDoS ataka	Paskirstytoji paslaugų trikdymo ataka
ENISA	Europos Sąjungos tinklų ir informacijos saugumo agentūra
ES	Europos Sąjunga
ECSO	Europos kibernetinio saugumo organizacija
ESBO	Europos saugumo ir bendradarbiavimo organizacija
FTTH	Plačiajuostė telekomunikacinė šviesolaidžio sistema, tiesiama iki konkretaus vartotojo namo
ISM	Interneto srauto mainai
IT	Informacinės technologijos
JAV	Jungtinės Amerikos Valstijos
JK	Jungtinė Karalystė
JTO	Jungtinių tautų organizacija
LR	Lietuvos Respublika
NATO	Šiaurės Atlanto Sutarties Organizacija
NR.	Numeris
PVZ.	Pavyzdžiui

ĮVADAS

Kibernetinio saugumo problemos kilo su elektroninės erdvės atsiradimu. Vis daugiau visuomeninių, dažnai labai svarbių santykių ir sistemų keliantis į elektroninę erdvę, kibernetinis saugumo aktualumas didėja. Tai nėra tik technologinė problema, nes didžiąją daugumą kibernetinio saugumo problemų sukuria ne technologijos, o žmonės; dažnai tai yra tyčiniai, gerai apgalvoti, tikslingai orientuoti į siekiamus tikslus, aukštos kvalifikacijos reikalaujantys veiksmai. Situaciją komplikuoja tai, kad į šiuos elektroninės erdvės santykius įsijungia ir valstybės, įskaitant labai galingas valstybes (Kinija, Rusija, JAV ir kitos) su didžiuliais resursais (įskaitant finansinius, žmogiškuosius ir kitokius resursus) ir, deja, neretai jų veikla sukelia neigiamas pasekmes. Daugumoje šalių kibernetinis saugumas priskiriamas prie kitų nacionalinių grėsmių (pvz.: fizinio karo grėsmė), todėl, autorių nuomone, kovos su kibernetinio saugumo pažeidimais priemonės, finansavimas, organizavimas ir kt. turi būti ne mažiau efektyvūs negu fizinėje erdvėje. Daugelis valstybių, suvokdamos problemų kompleksiškumą ir sudėtingumą, jau prieš kelis ar daugiau metų prisiėmė nacionalines kibernetinio saugumo strategijas, dalis iš jų jau spėjo jas atnaujinti ir priimti naujas strategijų redakcijas. Lietuva, deja, tokios strategijos neturi[2]. Susidariusi situacija ir buvo geras motyvas, pasitelkiant mokslinius tyrimo metodus, įvertinti sukauptą Europos Sąjungos bei NATO valstybių patirtį ir pasiūlyti modelį, leisiantį sukurti strategiją.

Tinkamam kibernetinio saugumo strategijos sukūrimui būtina įvertinti kitų šalių patirtį, atsižvelgti į atliktus mokslinius tyrimus bei doktriną. Lietuvos kibernetinio saugumo modelio sukūrimo tikslas buvo parengti tvirtus pagrindus kibernetinio saugumo strategijos rengimui. Kibernetinio saugumo modelis buvo kuriamas bei tyrimai atliekami projekto laikotarpiu nuo 2015 m. liepos mėn. iki 2017 m. kovo mėn., todėl projekte buvo vertinama šio laikotarpio užsienio šalių bei ekspertų patirtis, analizuojami tuo metu buvę šaltiniai. Kuriant aptariamą strategiją, būtina įvertinti laiko tarpą, praėjusį nuo šio projekto pabaigos iki strategijos sukūrimo. Baigiantis projektui, 2016 m. lapkričio mėn. 14d., ENISA paskelbė savo tyrimus kibernetinių nacionalinių strategijų srityje (NCSS Good Practice Guide: https://www.enisa.europa.eu/publications/ncss-good-practice-guide). Tai labai išsamus ir naudingas aukšto lygio ir didelės apimties darbas, atskleidžiantis šiuolaikinę kibernetinio saugumo strategijų problematiką. Svarstant ir kuriant naujas strategijas būtina atsižvelgti ir į šį dokumentą, jį taikyti sistemiškai atskirų šalių strategijose. Projekto grupės tikslas buvo sukurti ne bendro pobūdžio modelį (dalis tarptautinių ekspertų net neigė tokio universalaus modelio sukūrimo galimybę), bet, atlikus būtinus tyrimus, pasiūlyti Lietuvos Respublikai ir jos specifinei situacijai pritaikytą kibernetinio saugumo modelį. Projekto rezultatai turėtų būti naudingi visiems besidomintiems kibernetinio saugumo, jo reguliavimo klausimais, o ypač asmenims, kuriantiems ar prisidedantiems prie Lietuvos kibernetinio saugumo strategijos kūrimo.

2 Nuo 2011 m. Lietuvoje galioja „Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa“, kuri neatitinka strategijos požymių ir nelaikytina kibernetinio saugumo strategija.

1. MODELIO METODOLOGIJA IR BENDRIEJI PASTEBĖJIMAI DĖL MODELIO BEI STRATEGIJOS

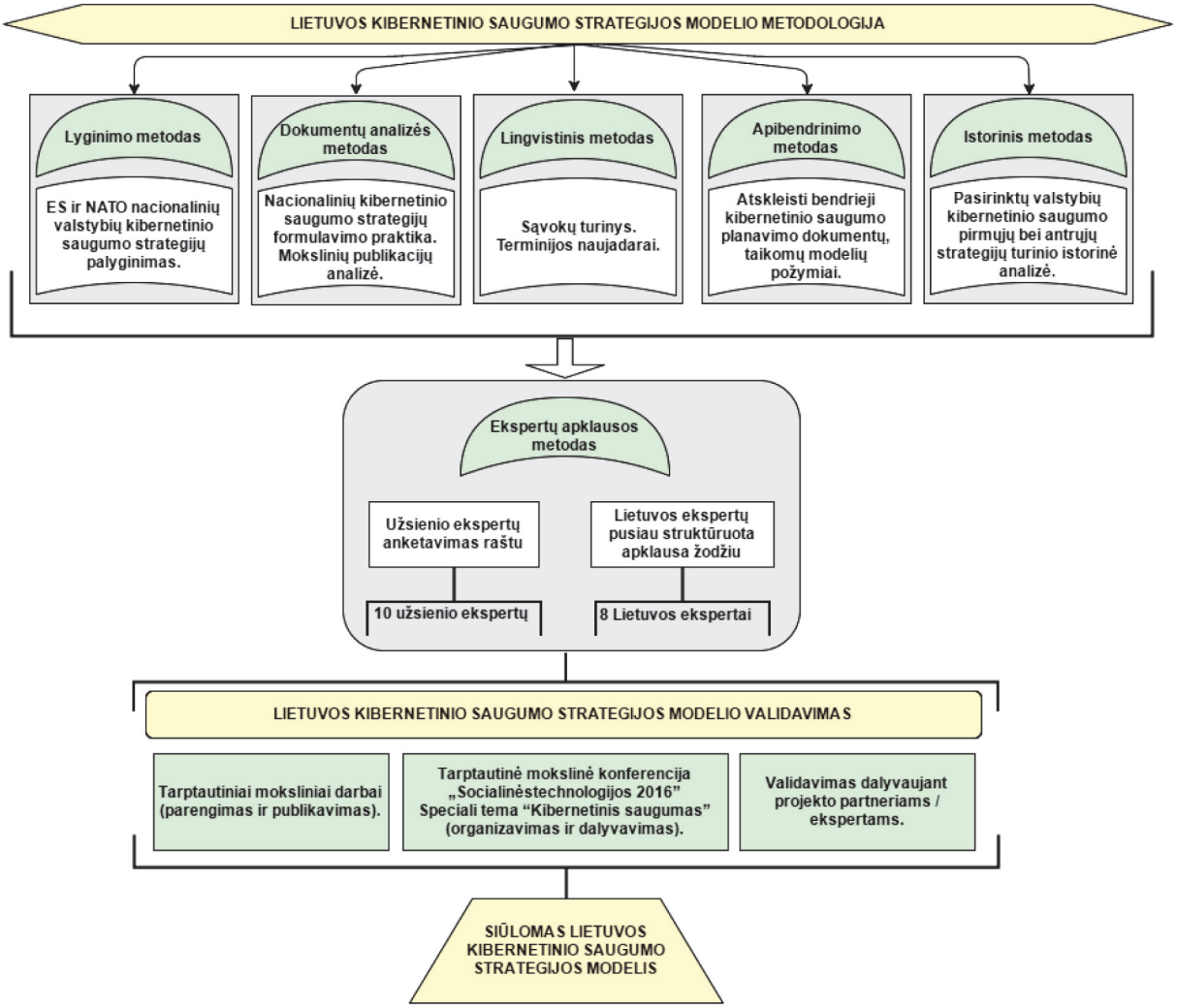
1.1. Lietuvos kibernetinio saugumo strategijos modelio metodologija

Kuriant Lietuvos kibernetinio saugumo strategijos modelį, buvo naudojamas kompleksas metodų / tyrimo ir modelio kūrimo įrankių, kuriuos galima sugrupuoti į tris grupes:

1. Literatūros ir dokumentų apžvalga;
2. Ekspertų apklausa;
3. Loginis modeliavimas, dalyvaujant vidinei projekto komandai.

Tyrimo metodologija atvaizduotina paveikslėlyje Nr. 1.

Paveikslėlis Nr. 1. *Autorių sudaryta tyrimo metodologija*



Lyginimo metodas. ES ir NATO nacionalinių valstybių kibernetinio saugumo strategijų palyginimas buvo atliekamas lyginant pagrindinius kriterijus[3] naujausiose galiojančiose atitinkamų valstybių kibernetinio saugumo strategijose. Palyginamieji kriterijai buvo nustatyti atliekant ES ir NATO strateginių kibernetinio saugumo dokumentų nuostatų palyginimą ir analizę, išskiriant abiem organizacijoms bendrai būdingas nuostatas.

Buvo lygintos ES ir NATO valstybių, lyginimo metu turinčių patvirtintas nacionalines kibernetinio saugumo strategijas, galiojančių strategijų nuostatos. Buvo lyginamos ir tų valstybių strategijos, kurios priklauso ES, bet nepriklauso NATO ir atvirkščiai. Apibendrinant, buvo lygintos šių valstybių kibernetinio saugumo strategijos[4]:

Lentelė Nr. 1. *Autorių sudarytas ES ir NATO valstybių, turinčių patvirtintas nacionalines kibernetinio saugumo strategijas, sąrašas.*

	ES valstybė	NATO valstybė	Bendras sąrašas
		Albanija	Albanija
	Austrija		Austrija
	Belgija	Belgija	Belgija
	Bulgarija	Bulgarija	Bulgarija
		Kanada	Kanada
	Kroatija	Kroatija	Kroatija
	Kipras		Kipras
	Čekijos Respublika	Čekijos Respublika	Čekijos Respublika
	Danija	Danija	Danija
	Estija	Estija	Estija
	Suomija		Suomija
	Prancūzija	Prancūzija	Prancūzija
	Vokietija	Vokietija	Vokietija
	Vengrija	Vengrija	Vengrija
	Airija	Airija	Airija

3 Autorių pasirinkti kriterijai apibendrintai: 1) principai, 2) bendradarbiavimas su privačiu sektoriumi, 3) kova su elektroniniais nusikaltimais, 4) kibernetinė gynyba, 5) moksliniai tyrimai, 6) standartai, 7) pagrindinių vertybių rėmimas, 8) „žaidėjų“ / institucijų užduotys bei kompetencija.

4 Dvi valstybės 2017 m. vasario mėnesį dar neturėjo nacionalinių kibernetinio saugumo strategijų: Graikija bei Švedija.

	ES valstybė	NATO valstybė	Bendras sąrašas
	Italija	Italija	Italija
	Latvija	Latvija	Latvija
	Lietuva	Lietuva	Lietuva
	Liuksemburgas	Liuksemburgas	Liuksemburgas
	Malta		Malta
	Olandija	Olandija	Olandija
		Norvegija	Norvegija
	Lenkija	Lenkija	Lenkija
	Portugalija	Portugalija	Portugalija
	Rumunija	Rumunija	Rumunija
	Slovakija	Slovakija	Slovakija
	Slovėnija	Slovėnija	Slovėnija
	Ispanija	Ispanija	Ispanija
		Turkija	Turkija
	Jungtinė Karalystė	Jungtinė Karalystė	Jungtinė Karalystė
		JAV	JAV

Turint omenyje nacionalines kibernetinio saugumo strategijas, nacionaliniu mastu visuomet gali būti skirtumų, dėl kurių skirsis ir pačios strategijos bei jų turinys, visgi, buvo prieita išvados, kad bendri strategijų elementai gali būti nagrinėjami. O identifikuoti skirtumai kaip tik gali atskleisti tam tikras tendencijas bei kitus rezultatus.

Paminėtina, kad eilės atliktų tyrimų apimtyje jau yra palygintos ES valstybių nacionalinės kibernetinio saugumo strategijas (ENISA, 2014[5]; BSA, 2015[6] ir kt.). Šie tyrimai atskleidė bendrus strategijų panašumus ir skirtumus. Tačiau ES ir NATO kibernetinio saugumo klausimų koordinavimo iniciatyvų bei atskirų valstybių kibernetinio saugumo strategijų nuostatų palyginimo iki šio palyginimo nebuvo atlikta.

ES ir NATO dokumentų ir atskirų ES ir NATO valstybių kibernetinio saugumo strategijų lyginamąja analize siekta nustatyti strategijų panašumus ir skirtumus, taip pat gerąją praktiką, kurią atskiros valstybės išvystė nacionaliniu lygiu.

5 An evaluation framework for Cyber Security Strategies, ENISA, 2014. Žiūrėta 2017 01 17 // https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1

6 EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace, BSA, 2015. Žiūrėta 2017 01 17 // http://cybersecurity.bsa.org/index.html

Istorinis metodas. Tyrimui pasirinktos valstybės, kuriose istoriniu aspektu kibernetinio saugumo strategijose yra pastebimas ženklus pokytis. Tyrimas buvo atliekamas nagrinėjant pasirinktų valstybių kibernetinio saugumo pirminių bei antrinių strategijų turinio istorinę analizę. Buvo vertinami kibernetinio saugumo strategijų sudedamieji elementai – grėsmės ir iššūkiai, principai, metodai, pagrindiniai tikslai, įgyvendinimas (jų istorinis kitimas). Tyrimui pasirinkti minėti elementai, nes būtent jie yra pastebimi kaip pagrindiniai sudedamieji tiek pirminių, tiek ir antrinių strategijų elementai ir šie elementai visapusiškai atskleidžia kibernetinio saugumo strategijų turinį. Tyrimo eigoje buvo vertinama, koks yra strategijų sudedamųjų elementų pokytis istorinėje eigoje, tiriama, kaip kito pasirinktų kibernetinio saugumo strategijų turinys, sprendžiami klausimai ir klausimų sprendimo būdai.

Tyrimo analizei buvo pasirinktos valstybės, priklausančios Europos Sąjungos bei NATO organizacijoms; tik NATO organizacijai bei tik Europos Sąjungai. Visų pirma, pasirinktos valstybės, priklausančios tiek Europos Sąjungai, tiek NATO – Olandija, Estija, Čekija. Visos šios valstybės yra priėmusios antrąsias kibernetinio saugumo strategijas. Antra, tolimesniam kibernetinio saugumo strategijų istorinės raidos palyginimui pasirinkta tik NATO valstybė – JAV. Ir trečia, pasirinkta ES šalis, nepriklausanti NATO organizacijai – Suomija. Toks skirtingas šalių priklausomumo lygis tarptautinėms organizacijoms atskleidė kibernetinio saugumo strategijų tendencijas, taip pat – parodė regionines kibernetinio saugumo perspektyvas.

Ekspertų apklausos metodas. Buvo atliktas kokybinis tyrimas, nes gilesnei reiškinio analizei reikalingos respondentų specifinės žinios ir patirtis. Kokybinio tyrimo strategija remiasi autorių Ritchie J ir Lewis J. siūlomais pavyzdžiais[7]. Tiriant kibernetinio saugumo strategijų modelius ekspertų žinių panaudojimas, pasitelkiant ekspertų apklausos metodą, yra naujausių mokslo žinių geriausia akumuliavimo galimybė.

Autoriai atliko dviejų lygių ekspertų apklausą:

1. užsienio ekspertų anketavimą raštu;
2. Lietuvos ekspertų pusiau struktūruotą apklausą žodžiu.

Atliekant ekspertų apklausą siekiant kokybiškų tyrimo rezultatų labai svarbu tinkamai parinkti apklausiamus ekspertus, todėl atsižvelgiant į tai, kad žinios yra itin specifinės, naujos bei apimančios skirtingas mokslų sritis, labai svarbu identifikuoti ir apklausti tinkamus ekspertus. Užsienio ekspertų atranką autoriai atliko pagal tiriamos srities išmanymą. Kadangi kibernetinis saugumas yra kartu ir kompleksinis reiškinys, tai šalia keleto šios srities specialistų, besispecializuojančių kibernetinio saugumo projektuose, tiriamą reiškinį gerai išmano ir asmenys, dirbantys IT teisės bei saugos technologijų srityse, todėl autoriai pasirinko ekspertus, gerai išmanančius elektroninės erdvės specifiką, elektroninių duomenų saugumą, asmens duomenų teisinį reguliavimą ir kitas su kibernetinio saugumo reiškiniu susijusias sritis. Renkant ekspertus buvo siekiama surasti vienodai aukštos kompetencijos ekspertus. Kitas svarbus ekspertų apklausos elementas yra tinkamas klausimų formulavimas, autoriai suformulavo 27 klausimus, apimančius esminius kibernetinio saugumo elementus. Klausimai buvo formuluojami remiantis autoriaus Ritchie J. ir Lewis J. pateikiama klausimų formulavimo metodologija[8]. Užsienio ekspertams buvo pateikti atviri klausimai siekiant gauti jų laisvą vertinimą, pasitelkiant jų sukauptas žinias ir intuiciją.

Parengtos anketos, kuriose vyrauja atviri klausimai, buvo išsiųstos pasirinktiems ekspertams elektroniniu paštu arba per socialinį tinklą Linkedin. Ekspertai anketas pildė neribojami laiko, pertraukų ar pildymo vietos, todėl galėjo geriau apgalvoti klausimus, juos užpildyti išsamiau. Atsižvelgiant į tai, kad elektroninių apklausų vienas iš trūkumų yra nepakankamas anketų užpildymas, autoriai taikė pakartotinius

7 Ritchie J. ir Lewis J. *Qualitative Research Practice: A Guide for Social Science Students and Researchers.* Sage, 2003. P.77–85.

8 Ten pat. P.153–155.

priminimus elektroninių paštu. Aptariamo objekto elektroninis ekspertų anketavimas turi ir kitų trūkumų, pavyzdžiui, dėl tiriamo objekto kompleksiškumo poreikis ekspertui turėti platų spektrą žinių, kurio vienas asmuo gali neturėti, arba atsakydamas į klausimus ekspertas daliai klausimų gali turėti mažiau gilias žinias negu kitais klausiamais, į tai autoriai atsižvelgė vertindami ekspertų atsakymus. Atsižvelgiant į tai, kad kibernetinio saugumo reiškinys yra kompleksinio pobūdžio ir dalį aspektų ekspertai nėra atskirai tyrinėję, todėl normalu, kad dalies klausimų pavieniai ekspertai negalėjo atsakyti.

Autoriai pasirinko ekspertinę imtį, t.y. 10 užsienio ekspertų, turinčius žinių ir patirties kibernetinio saugumo srityje. Autoriai vertino ekspertų nuomones apibendrindami gautus apklausos rezultatus iš individualaus užsienio ekspertų anketavimo. Šios ekspertų nuomonės toliau pateikiamos nagrinėjant nacionalinių kibernetinio saugumo strategijų skirtumus bei tipinio unifikuotos kibernetinio saugumo strategijos modelio galimybę.

Buvo apklausti šie užsienio ekspertai: Samantha Adams (Nyderlandų Karalystė), Lorenzo Dalla Corte (Italija), Sintija Deruma (Latvijos Respublika), Uldis Kinis (Latvijos Respublika), Jesus Maria Gonzalez Perez (Ispanija), Anna Sarri (Graikija, ENISA), Dimitra Liveri (Graikija, ENISA), Johan Stronkhorst (Belgija), Jaan Priisalu (Estija), Ferenc Szalai (Vengrija), Kadri Kaska (Estija). Ekspertų aprašymas pridedamas priede Nr. 1. Klausimai užsienio ekspertams ir užsienio ekspertų atsakymai pateikiami priede Nr. 2.

Lietuvos ekspertų apklausai autoriai pasirinko Lietuvoje gyvenančius ir dirbančius ekspertus, turinčius žinių ir profesinės patirties kibernetinio saugumo srityje. Lietuvos ekspertai buvo apklausiami pagal pusiau struktūruoto interviu scenarijų. Pusiau struktūruotiems giluminiams interviu iš anksto buvo sukurtas bendras klausimynas, kuriame pateikti patys svarbiausi, esminiai klausimai dėl kibernetinio saugumo strategijų ir jų pritaikymo Lietuvos aplinkai. Tačiau, interviu eigoje, reaguodami į ekspertų atsakymus ir komentarus, autoriai uždavė ir papildomų, iš anksto neparengtų klausimų. Tokiu būdu buvo siekiama išgauti kuo daugiau duomenų tiriama tema laisvo pokalbio metu. Apklausiant Lietuvos ekspertus buvo naudojami užrašai, kuriuose autoriai pasižymėjo aktualiausius ekspertų pabrėžiamus teiginius, komentarus ir savo pastabas. Duomenų giluminė analizė (angl. *in depth analysis*) pradedama tik užbaigus visų asmenų apklausas[9]. Kadangi pusiau struktūruotas interviu buvo pasirinktas kaip papildomas metodas duomenims išgauti, buvo apklausiamas sąlyginai mažas Lietuvos ekspertų skaičius – 8.

Lietuvos ekspertų apklausa buvo vykdoma žodžiu gyvai arba telefonu.

Autoriai vertino ekspertų nuomones apibendrindami gautus apklausos rezultatus iš individualaus užsienio ekspertų anketavimo ir Lietuvos ekspertų žodinės apklausos. Duomenys buvo struktūruojami atsižvelgiant į teminius autorių išskiriamus minčių junginius[10].

Buvo apklausti sekantys lietuvių ekspertai: Vytautas Butrimas (LR Krašto apsaugos ministerija), Algirdas Kunčinas (LR Asmens duomenų apsaugos inspekcija), Renata Mačiulevičienė (LR Informatikos ir ryšių departamentas prie vidaus reikalų ministerijos), Rytis Rainys, (Ryšių reguliavimo tarnyba), Vitalij Dmitrijev (LR Seimas), Arvydas Plėštys (LR Krašto apsaugos ministerija), Marius Pareščius (International security cluster), Saulius Japertas (Kauno technologijos universitetas). Ekspertų aprašymas pridedamas priede Nr. 2. Kadangi Lietuvos ekspertų apklausa buvo vykdoma žodžiu gyvai ir telefonu, ekspertų atsakymai nepateikiami, tačiau jie buvo užfiksuoti ir panaudoti kuriant modelį.

Dokumentų analizės metodas. Taip pat buvo pasitelktas empirinis dokumentų analizės metodas. Jis taikytas apibendrinant nacionalinių kibernetinio saugumo strategijų formulavimo praktiką, išryškinant ten-

9 Irving Seidmen. *Interviewing as Qualitative Research: A Guide for Researchers in Education and Social sciences*. Teachers College, Columbia University, New York and London, Forth edition. 2005. P.113.

10 Ten pat. P. 125.

dencijas, strategijų atitinkamų struktūrinių dalių nuostatų formulavimo variantus. Tyrime analizuotos ES ir NATO valstybių nacionalinės kibernetinio saugumo strategijos, susiję dokumentai, taip pat ES ir NATO nepriklausančių valstybių kibernetinio saugumo strategijos.

Apibendrinimo metodas. Nagrinėjami klausimai lėmė, kad tyrime buvo būtina susieti kibernetinio saugumo strateginio planavimo ir kibernetinio planavimo bei kibernetinio saugumo teisinio reguliavimo sritis, įskaitant skirtingas praktikas ES ir NATO bei atskirose nacionalinėse valstybėse. Siekiant atskleisti bendruosius kibernetinio saugumo planavimo dokumentų, taikomų modelių požymius, taikytas apibendrinimo metodas.

Lingvistinis metodas. Šis metodas buvo reikšmingas atskleidžiant sąvokų turinį, taip pat tiriant terminijos naujadarus. Atliekant tyrimą, buvo susidurta su regioniniuose bei atskirų valstybių dokumentuose naudojamomis skirtingomis sąvokomis, todėl sąvokų interpretavimas taip pat buvo svarbus kuriant Lietuvos nacionalinės kibernetinio saugumo strategijos modelį.

Kiti metodai. Loginės analizės, sisteminės analizės, sintezės, dedukcinis tyrimo metodai buvo naudojami viso tyrimo metu. Remiantis jais nuosekliai buvo tiriami strateginiai kibernetinio saugumo dokumentai tiek regioniniu mastu (ES ir NATO), tiek atskirose valstybėse. Buvo sistemiškai analizuojami mokslinės literatūros, doktrinos ir kiti šaltiniai, įskaitant norminius teisės aktus, informacinius ir statistinius duomenis. Šių metodų naudojimas leido struktūriškai jungti argumentus, grupuoti nagrinėjamas problemas ir jų sprendimo būdus, suformuoti modelio koncepciją.

Tyrimų rezultatai buvo aptarti bei aprobuoti tarptautinės mokslinės konferencijos metu: 2016 m. rugsėjo 29–30 dienomis Mykolo Romerio universitete vyko tarptautinė mokslinė konferencija „Socialinės technologijos`2016“, o šios konferencijos speciali tema buvo „kibernetinis saugumas“. Bendroji nuoroda į konferenciją: http://soctech16.mruni.eu/ Taip pat, papildomai tyrimų rezultatai buvo aptarti su kai kuriais mokslinės konferencijos dalyviais-ekspertais atskiro konferencijos dalyvių ir tyrimo grupės nariais metu.

Tyrimo rezultatai buvo validuoti publikuojant mokslinius straipsnius tarptautiniuose mokslo žurnaluose. Tyrimo grupės nariai savo tyrimus dėl kibernetinio saugumo strategijų publikavo šiuose mokslo straipsniuose recenzuojamuose tarptautiniuose mokslo žurnaluose, įtrauktuose į Web of Science bei SCOPUS duomenų bazes:

Štitilis D., Pakutinskas P., Laurinaitis M., Malinauskaitė I. A model for the national cyber security strategy. The lithuanian case // Journal of Security and Sustainability Issues, Volume 6 Number 3, March, 2017

Štitilis D., Pakutinskas P., Malinauskaitė I., Kinis U. Concepts and principles of cyber security strategies // Journal of Security and Sustainability Issues, Volume 6 Number 2, December, 2016;

Štitilis D., Pakutinskas P., Malinauskaitė I. Preconditions of sustainable ecosystem: cyber security policy and strategies // Entrepreneurship and Sustainability Issues, Volume 4, Number 2, December, 2016;

Štitilis D., Pakutinskas P., Malinauskaitė I. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis // Security Journal, October, 2016, p. 1–18.

Dar vienas straipsnis „Suggested Areas of Unified (International) Cyber Security Strategy and National Cyber Security Strategy” buvo parengtas, priduotas ir priimtas spausdinimui recenzuojamuose tarptautiniuose mokslo žurnale, įtrauktame į Web of Science duomenų bazę „International Journal of Critical Infrastructure Protection” (Impact factor 1.351). Šis straipsnis turėtų būti išspausdintas 2017 m. pirmojoje pusėje.

Publikuotų straipsnių kopijos pridedamos priede Nr. 3.

1.2. Bendrieji pastebėjimai dėl Lietuvos kibernetinio saugumo strategijos modelio bei strategijos

Remiantis autorių atliktais lyginamuoju, istoriniu, ekspertų apklausos ir kitais tyrimais, taip pat pasitelkiant geriausią kitų valstybių praktiką, toliau pateikiami Lietuvos nacionalinės kibernetinio saugumo strategijos modelio elementai, taip pat pateikiamos gairės dėl šių Lietuvos kibernetinio saugumo strategijos sudedamųjų dalių turinio.

Autorių sukurtas modelis yra orientuotas į naujos, šiuolaikiškos Lietuvos kibernetinio saugumo strategijos sukūrimą. Šiuolaikinis kibernetinio saugumo strategijos modelis kiekvienai valstybei, o šiuo konkrečiu atveju – Lietuvos Respublikai – gali padėti susitelkti į pagrindinius ir esminius kibernetinio saugumo ir atsparumo gerinimo ir užtikrinimo klausimus. Šiuo laikinė kibernetinio saugumo strategija gali ne tik teigiamai įtakoti kibernetinio saugumo užtikrinimą valstybėje. Tokios strategijos egzistavimas ir tinkamas įgyvendinimas gali padėti spręsti atitinkamos valstybės nacionalinio saugumo ar kitus aktualius klausimus, užtikrinti tinkamą modernios visuomenės vystymąsi.

Autorių pasirinktas nacionalinės kibernetinio saugumo strategijos modelis yra aukšto lygio planavimo dokumentas, apibrėžiantis pagrindinius tikslus ir pagrindines priemones atitinkamai valstybei kibernetinio saugumo srityje. Pasirinkus tokį modelio tipą, dar svarbiau turėti ir konkrečias įgyvendinimo nuostatas. Tokios nuostatos gali būti integruotos ir į nacionalinę strategiją, ir pateikiamos kaip atskiras dokumentas. Autorių nuomone, priemonių planas Lietuvoje galėtų būti kaip atskiras dokumentas, kadangi priemonių plano peržiūra turėtų būti vykdoma dažniau nei pačios strategijos.

Labai svarbu yra strategijos galiojimas. Remiantis atlikto tyrimo rezultatais, strategija turėtų galioti iki 5 metų, tačiau, taip pat turėtų būti peržiūrima ir dažniau. Taip būtų reaguojama, pavyzdžiui, į technologijų, kurios taikomos užtikrinant kibernetinį saugumą, pokyčius. Tuo atveju, jei be strategijos būtų tvirtinamas strategijos įgyvendinimo veiksmų, šis planas turėtų būti peržiūrimas kas metus. Ekspertų buvo nurodyta, kad detalės greitai sensta, todėl dar ir dėl to būtina peržiūrėti periodiškai nustatytu laiku.

Atkreiptinas dėmesys, kad pagal modelį kuriama kibernetinio saugumo strategija, be kitų funkcijų, turėtų būti pagrindinis dokumentas formuoti terminus ir terminologiją kibernetinio saugumo srityje. Šiai dienai terminai įvairiuose dokumentuose / teisės aktuose iš esmės skiriasi, nesutampa, prieštarauja, dalinai suformuluoti netinkamai. Tokia situacija taisytina. Lietuvos kibernetinio saugumo strategija taip pat turėtų kelti tikslą formuoti sąvokas kibernetinio saugumo srityje ir turėtų būti kaip pirminis šaltinis, kuriuo remtųsi visi kiti šaltiniai, reguliuodami ir reglamentuodami su kibernetiniu saugumu susijusius santykius.

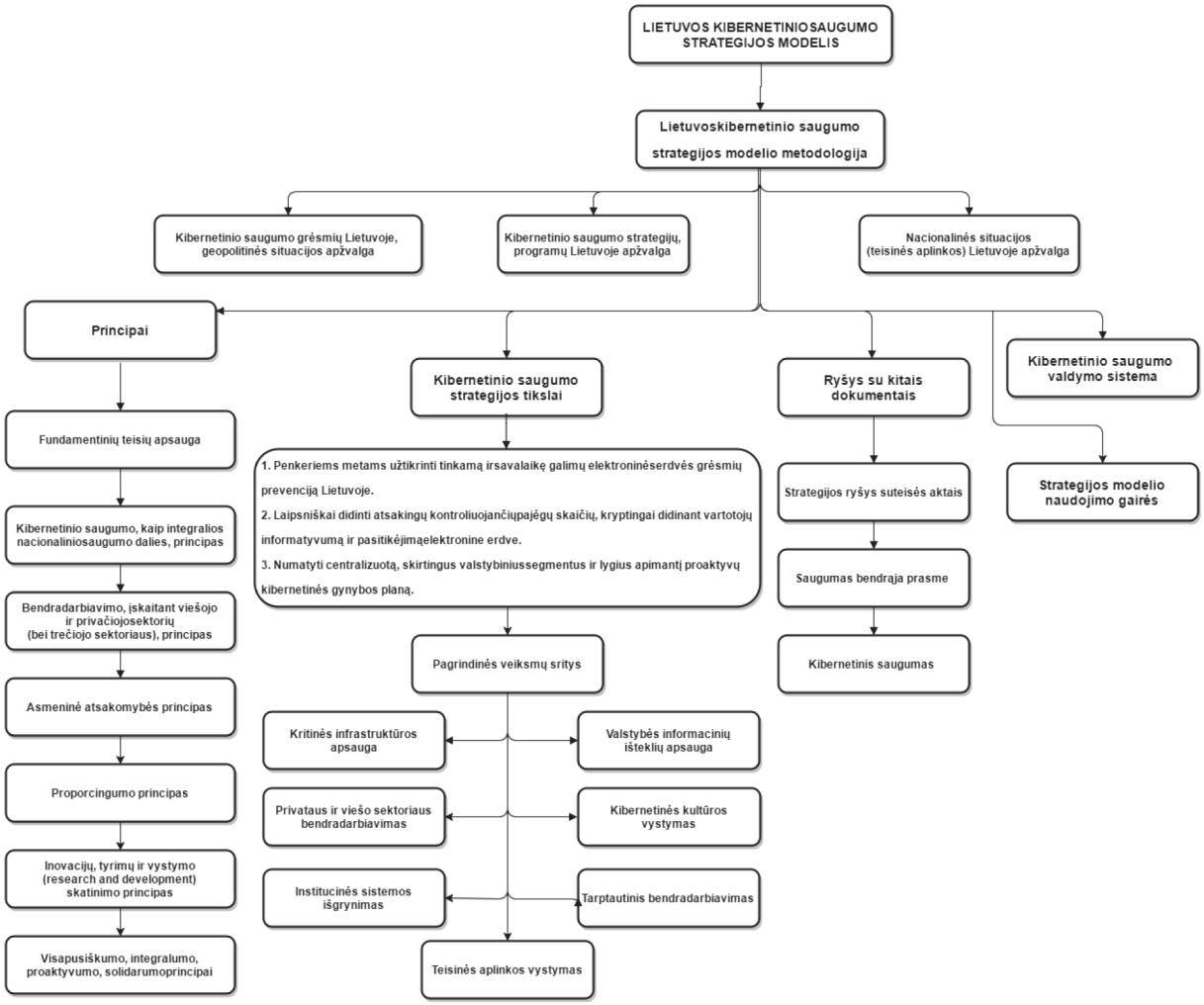
Pažymėtina, kad sąvokos labai svarbios ne tik rengiant nacionalinę kibernetinio saugumo strategiją, ne tik nacionalinės kibernetinio saugumo strategijos kontekste, bet ir plačiame kontekste. Sąvokos nacionalinėje kibernetinio saugumo strategijoje turi sukurti pagrindą vienodam ir sisteminiam sąvokų kibernetinio saugumo srityje naudojimui kituose valstybės dokumentuose, pradedant LR kibernetinio saugumo įstatymui ir baigiant lydimaisiais teisės aktais. Nacionalinė kibernetinio saugumo strategijoje pateikiamos sąvokos turi būti pagrindu ir pavyzdžiu formuojant ir naudojant sąvokas kituose dokumentuose. Tik taip galima užtikrinti nuoseklų sąvokų panaudojimą, išvengti prieštaravimų sąvokose bei išvengti problemų, kurios gali kilti dėl netinkamų, nekokybiškų ar prieštaraujančių savokų naudojimo.

Sąvokos kibernetinio saugumo srityje turėtų atitikti technologinio neutralumo, funkcinio ekvivalentiškumo ir kitus susijusius principus, būti neperkrautos gramatiškai pertekline informacija. Keletas sąvokų, kaip pavyzdžiai, yra pateikiama ir šio modelio pradžioje.

Autorių atlikta kibernetinio saugumo strategijų ir jų tvirtinimo atskirose valstybėse analizė parodė, kad nepaisant to, jog kai kuriose valstybėse (tokių valstybių mažuma) tokios strategijos yra patvirtintos kaip teisės aktai (iš jų ir Lietuvoje), visgi, strategijos neturi visų teisės akto požymių ir laikytinos kaip strateginiai planavimo dokumentai. Šie rezultatai atskleisti ir šioje autorių išspausdintoje mokslinėje publikacijoje: Štitilis D., Pakutinskas P., Malinauskaitė I., Kinis U. Concepts and principles of cyber security strategies // Journal of Security and Sustainability Issues, Volume 6 Number 2, December, 2016. Atsižvelgiant į tai, žemiau pateikiamas modelis gali būti laikomas teisinio reguliavimo koncepcija tik ta apimtimi, kad kibernetinio saugumo strategija gali būti tvirtinama teisės aktu – Seimo nutarimu ar Vyriausybės nutarimu. Tačiau tai nepanaikina to fakto, kad Lietuvos kibernetinio saugumo strategija turėtų būti laikoma strateginiu planavimo dokumentu, o ne teisės aktu, sukuriančiu konkrečias teises ir pareigas, kurių nevykdymas užtraukia atsakomybę.

Remiantis autorių atliktais tyrimais, visuminė Lietuvos kibernetinio saugumo strategijos modelio vizualizacija pateikiama žemiau.

Paveikslėlis Nr. 2. *Autorių sudaryta Lietuvos kibernetinio saugumo Strategijos modelio vizualizacija*



Toliau yra nagrinėjamos ir analizuojamos atitinkamos modelio dalys / institutai.

2. LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO SITUACIJOS APŽVALGA

Kuriant nacionalinę kibernetinio saugumo strategiją, reikia atsižvelgti į nacionalinę situaciją. Autoriai išskiria šiuos pagrindinius nacionalinės Lietuvos situacijos elementus:

- Kibernetinės grėsmės Lietuvoje, geopolitinė situacija;
- E-viešosios ir e-verslo paslaugos Lietuvoje;
- Nacionalinė situacija, susijusi su teisine aplinka, įskaitant nacionalines programas, strategijas, susijusias su IT saugumu, elektroninės informacijos sauga.

2.1. Kibernetinio saugumo grėsmių ir geopolitinės situacijos Lietuvos Respublikoje apžvalga

Remiantis Valstybės saugumo departamento bei Krašto apsaugos ministerijos duomenimis[11], 2015 m. saugumo situacija Lietuvos kaimynystėje ir visame regione išliko įtempta: toliau augo Rusijos imperinės ambicijos, didėjo jos užsienio politikos agresyvumas. Karinės jėgos reikšmė bendrajai saugumo situacijai Rytų Europoje ir konkrečių šalių saugumui, labai padidėjusi 2014– 2015 m. dėl agresyvių Rusijos veiksmų Ukrainoje, išlieka ypač didelė. Be to, 2015 m. saugumo situacijos Rytų Europoje klausimą ėmė gožti kova su terorizmu ir migracijos krizė. Šie klausimai yra vieni svarbiausių Europos Sąjungos (toliau – ES), NATO ir daugelio valstybių darbotvarkėje ir 2016 m.

Tos pačios studijos duomenimis[12], kibernetinis šnipinėjimas, atakos (DDoS atakos, vartotojų sąsajų pakeitimai ir kt.), kibernetinė žvalgyba (skenavimai) – dažniausiai 2015 m. fiksuota veikla elektroninėje erdvėje, nukreipta prieš Lietuvos valstybės institucijas, strateginę reikšmę šalies nacionaliniam saugumui turinčius objektus ir privatų sektorių. 2015 m. pastebėta, kad finansiškai motyvuoti elektroniniai įsibrovėliai siekia ne tik ekonominės, bet ir politinės naudos. 2015 m. nustatyta dar viena tendencija, kai tikrieji kenkėjiško kodo kūrėjai ir platintojai vis labiau naudoja įvairias priemones ir resursus užsimaskuoti ir pasislėpti, t. y. likti neidentifikuoti arba klaidingai identifikuoti: į programinį kodą įterpiami „pavogti parašai“, programinio kodo dalys, kurios slepia tikrąją kenkėjiško kodo paskirtį. Tokiu būdu, turint omenyje tiek finansinį, tiek ir politinį kontekstą, kibernetinis šnipinėjimas prieš Lietuvos valstybės institucijas, šalies kritinės infrastruktūros objektus, privatųjį sektorių išlieka viena pagrindinių grėsmių šalies nacionaliniam saugumui. Atliktos studijos duomenimis[13], 2015 m. identifikuotos grėsmingiausios įmonės Lietuvos Respublikai siejamos su Rusija, Kinija, Indija ir Iranu. Kibernetinio ginklo požymiai buvo aptikti tiek Lietuvos valstybės institucijų, šalies kritinės infrastruktūros objektų tinkluose ir sistemose, tiek privataus sektoriaus galiniuose įrenginiuose. Didžiausią grėsmę šalies nacionaliniam saugumui kaip ir pastaraisiais metais kėlė su Rusija susiję elektroniniai įsibrovėliai, įskaitant Rusijos žvalgybos ir saugumo tarnybas.

Taigi, bene svarbiausia yra apsaugoti kritinę infrastruktūrą. Atskiras dėmesys taip pat turėtų būti skiriamas pramoninių procesų valdymo sistemoms. Tokių sistemų saugumo užtikrinimo klausimas šiuo metu keliamas kaip vienas iš prioritetų nemažos dalies ES ir pasaulio valstybių strategijose gynybos kontekste. Lietuvos kontekste ypač aktualios SCADA sistemos, kurios Lietuvoje naudojamos, ir kurių pažeidžiamumas didėja.

11 Grėsmių nacionaliniam saugumui vertinimas. Lietuvos Respublikos Valstybės saugumo departamentas ir antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, Vilnius, 2016. Žiūrėta 2016 09 26// http://www.vsd.lt/Files/Documents/635948635773762500.pdf.

12 Ten pat.

13 Ten pat.

Viešosios e-paslaugos ir jų specifika Lietuvoje.

Pasinaudodamos interneto teikiamomis galimybėmis, valdžios ir verslo institucijos kasmet pasiūlo naujų e. paslaugų.

Šiuo tikslu sukurtas valdžios teikiamų e. paslaugų portalas – Elektroniniai valdžios vartai, pasiekiami adresu *www.epaslaugos.lt*. Portale, kurį administruoja Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos, galima rasti informaciją ir nuorodas į visas svarbiausias Lietuvoje teikiamas viešąsias ir administracines e. paslaugas. Dalį jų galima užsisakyti pačiame portale, o jei paslauga užsakoma tik jos teikėjo tinklapyje, į jį vartotojas nukreipiamas automatiškai.

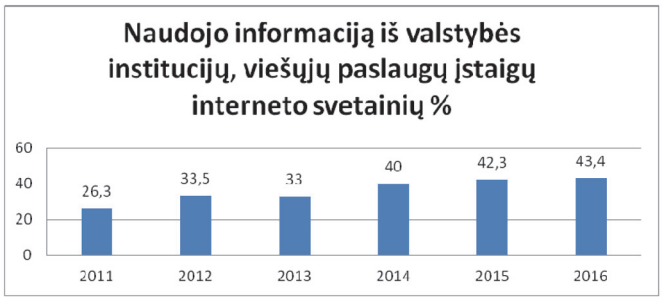
Tokiu būdu Lietuvos vartotojai gali pildyti deklaracijas elektroniniu būdu, pateikti įvairiausius prašymus valstybės institucijoms internetu. Patogu tai, jog valstybės ir privačios institucijos, bendradarbiaudamos tarpusavyje jau būna pateikusios dalį duomenų į gyventojui reikalingas užpildyti formas.

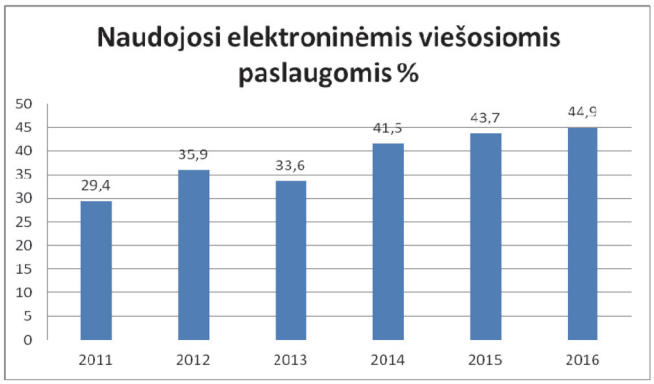
2015 m. birželį startavo e-sveikatos projektas, pagal kurį yra centralizuota sveikatos apsaugos sistema, apjungusi internetiniu būdu visas LR sveikatos apsaugos institucijas. Gyventojams suteikiama galimybė stebėti savo ligos istoriją, tyrimus, gauti vizito lapelį pas gydytoją. Visapusiškai įsigalioti naujoji e-sveikatos sistema turėtų nuo 2018 m. I ketvirčio.

2015 m. ES duomenimis, maudojimąsis elektroninės valdžios paslaugomis Lietuvos Respublikoje yra žemesnis nei ES vidurkis – žemas – 44 %, 31 % gyventojų pildė elektronines paslaugų formas internete[14].

Per 2016 m. informaciją iš valstybės institucijų interneto svetainių naudojo 65,9 proc. įmonių (2015m. – 71 proc.). Informaciją naudojo įmonės komercinei veiklai, administravimo procesams, elektroninėms paslaugoms kurti ar teikti. Bent kartą per metus valstybės institucijų ar kitų viešųjų paslaugų įstaigų elektroninėmis paslaugomis pasinaudojo 60 proc. 16–74 metų amžiaus žmonių, jie ieškojo informacijos įstaigų interneto svetainėse, pildė ir pateikė oficialius blankus tiesiogiai internete.

Paveikslėlis Nr. 3. *Naudojamasis viešosiomis paslaugomis Lietuvoje. Sudaryta remiantis LR statistikos departamento duomenimis.*





Lietuvoje yra sukurta reikalinga infrastruktūra ir įstatymai elektroninei komercijai vystyti. 2000 m. priimtas elektroninio parašo įstatymas. 2015 m. kvalifikuotų sertifikatų sudarymo paslaugas Lietuvos Respublikoje teikė ir buvo prižiūrimi trys Lietuvos Respublikoje įregistruoti sertifikavimo paslaugų teikėjai: UAB Skaitmeninio sertifikavimo centras, VĮ Registrų centras, Gyventojų registro tarnyba. Palyginti su 2014 m., bendras Lietuvos sertifikavimo paslaugų tekėjų išduotų galiojančių kvalifikuotų sertifikatų skaičius 2015

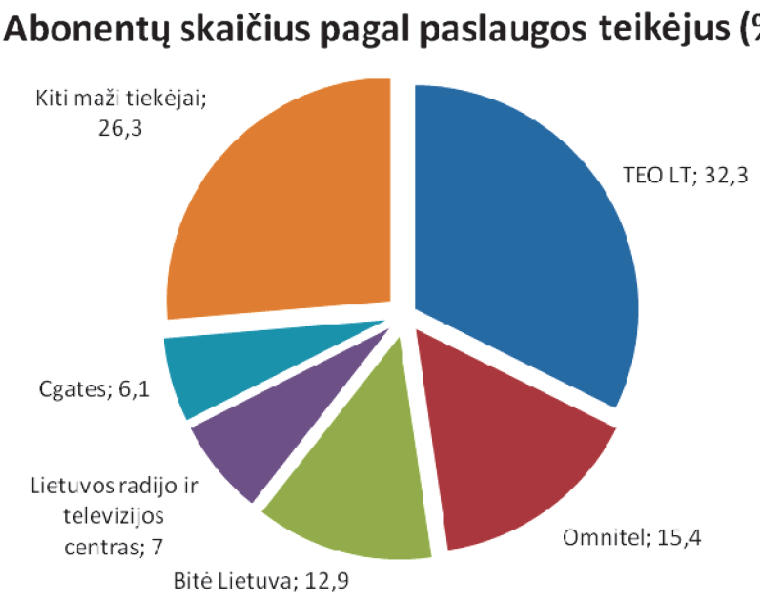
14 Digital Single Market. Country profile for Lithuania, eGovernment indicators. European Commission, 2017. Žiūrėta 2017 03 02 // https://digital-agenda-data.eu/charts/country-profiles-the-relative-position-against-all-other-european-countries#chart={%22indicator-group%22:%22egovernment%22,%22ref-area%22:%22LT%22,%22time-period%22:%222015%22}

m. pab. padidėjo 7,45 proc. Atsižvelgiant į nuoseklų išduodamų kvalifikuotų sertifikatų skaičiaus augimą, darytina išvada, kad asmenų susidomėjimas elektroninio parašo panaudojimo galimybėmis pastebimai auga. Pagrindinės to priežastys, manytina, yra esamos pakankamos teisinės prielaidos naudoti elektroninį parašą ir plačiai naudojamų viešųjų paslaugų perkėlimas į elektroninę erdvę[15].

E-verslo paslaugos ir jų specifika Lietuvoje.

Viena iš svarbiausių paslaugų – interneto prieigos paslauga. Plačiajuosčio interneto prieigą Lietuvoje 2016 m. II ketvirtį teikė 102 ūkio subjektai. 2016 m. birželio 30 d. duomenimis Lietuvoje buvo 1,22 milijono plačiajuosčio interneto prieigos abonentų. Iš minėto skaičiaus 75,7 proc. sudarė namuose turintys interneto prieigą vartotojai (bendras plačiajuosčio ryšio abonentų skaičius – 845,6 tūkst., iš šio skaičiaus net 62,1 proc. naudojosi šviesolaidinėmis ryšio linijomis, mažmeninėmis interneto prieigos paslaugomis). Lietuva pirmauja ES šalyse. "In terms of penetration Lithuania is still number one in the ranking with a penetration rate of 36.8%, Latvia (36.2%) and Sweden (35.2%)."[16] Remiantis FTTH Global Ranking – end-September 2015, Lietuva šviesolaidinio ryšio tinklo skvarboje yra 9 vietoje pasaulyje.[17] Labai svarbu tai, kad didžioji dalis mažmeninių interneto prieigos paslaugų rinkos, matuojant vartotojų skaičiumi, priklauso vienai kompanijai, TEO LT teikė interneto prieigos paslaugas 39,4 proc. visų interneto prieigos vartotojų. TEO LT grupei priklausanti įmonė Omnitel užima antrą vietą mažmeninių interneto prieigos paslaugų teikėjų sąraše, matuojant abonentų skaičiumi, aptarnaudama 15,4 proc. visų klientų. Taigi šios dvi susijusios privataus verslo įmonės aptarnauja beveik 50 % Lietuvos interneto vartotojų. Kibernetinio saugumo incidento atveju, nukreiptu prieš šias dvi kompanijas, sutriktų didžiausia dalis teikiamų interneto paslaugų Lietuvoje. Dėl to būtina užtikrinti deramą institucijų bendradarbiavimą, siekiant užkirsti bet kokias galimas grėsmes.

Paveikslėlis Nr. 4. *Abonentų skaičius pagal paslaugos teikėjus. Sudaryta remiantis Ryšių reguliavimo tarnybos duomenimis.*



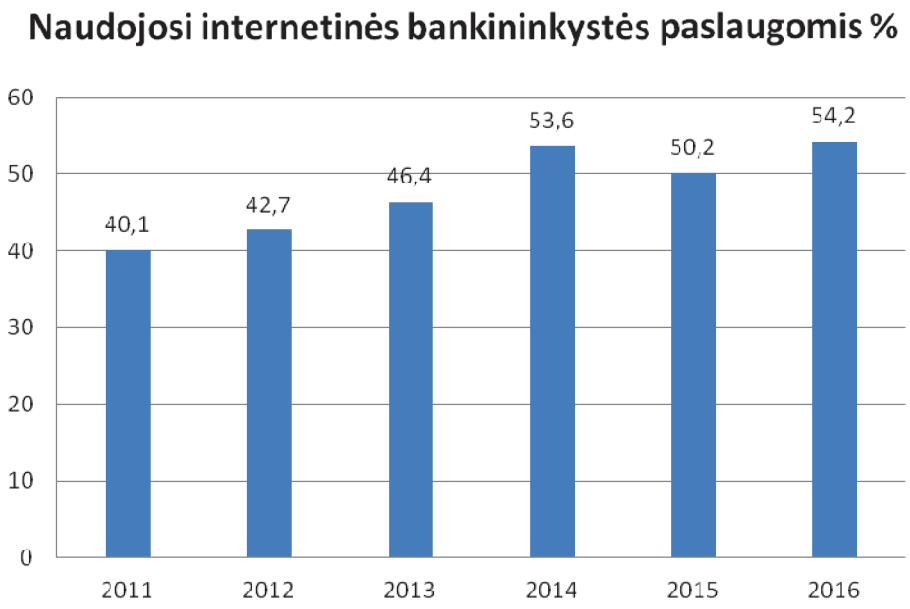
15 Ryšių reguliavimo tarnybos 2016 06 30 LR Elektroninio parašo įstatymo įgyvendinimo 2015 metų ataskaita, Ryšių reguliavimo tarnyba, 2016. Žiūrėta 2017 01 20 // http://www.rrt.lt/lt/apzvalgos-ir-ataskaitos/elektroninio-paraso-istatymo-1b73.html

16 Breaking news from the FTTH Conference 2016: Croatia, germany and Poland join the FTTH ranking. Fibre to the home conference "Calling for a brigher future", Council Europe, 2016. Žiūrėta 2016 06 20 // http://www.ftthcouncil.eu/documents/PressReleases/2016/PR20160217_FTTHranking_panorama_award.pdf

17 Fibre to the home conference "Calling for a brigher future", Council Europe, 2016. Žiūrėta 2016 06 20 // http://www.ftthconference.eu/images/Banners/Conference2016/Media%20downloads/20160217PressConference_presentation.pdf

Elektroninė bankininkystė ir bankų programėlės mobiliesiems įrenginiams populiarėja, keičiasi žmonių poreikiai. Naujosioms technologijoms paprastėjant, jos tampa prieinamos vis didesniam skaičiui žmonių. Be to, vartotojai yra praktiški ir supranta, kad elektroniniai įrankiai padeda sutaupyti laiko bei pinigų. LR statistikos departamento duomenimis 2016 m. daugiau kaip 54% žmonių naudojasi el. bankininkystės paslaugomis. LR Nacionalinės mokėjimų strategijoje numatoma veikti svarbiomis kryptimis, išplėtoti infrastruktūrą, sudaryti sąlygas masiškam bekontakčių ir momentinių mokėjimų naudojimui, stiprinti mokėjimo paslaugų naudotojų pasitikėjimą elektroniniais mokėjimais ir skatinti įpročius jais naudotis. Kritinė masė vartotojų jau naudojasi šiomis paslaugomis, dėl to bet koks išorinis trikdis darytų stipriai juntamą poveikį finansiniam aktyvumui.

Paveikslėlis Nr. 5. *El. bankininkystės naudotojų augimas. Sudaryta remiantis LR statistikos departamento duomenimis.*



Lietuvos banko duomenimis taip pat sparčiai daugėja gyventojų, naudojančių mobilųjį telefoną kasdieniams mokėjimams[18].

E. parašas privačiajame sektoriuje naudojamas bankuose – operacijoms, sutartims pasirašyti (panaudotų kvalifikuotų sertifikatų skaičius visuose informaciją pateikusiuose bankuose augo); verslo įmonėse – 2015 m. 86,4 proc. šalies gamybos ir paslaugų įmonių naudojosi e. parašu (2014 m. – 87,1 proc., 2013 m. – 85,8 proc.)[19].

Kiti duomenys.

Lietuvos Statistikos departamento duomenimis, 2016 m. pirmąjį ketvirtį asmeninius kompiuterius namuose turėjo 72 proc., interneto prieigą – 73 proc. namų ūkių. Palyginti su 2015 m., tai yra atitinkamai 4 ir 5 procentiniais punktais daugiau. Beveik visi (99 proc.) namų ūkiai, turintys namuose interneto prieigą, naudojosi plačiajuosčiu ryšiu. 88 proc. interneto prieigą turinčių namų ūkių naudojosi plačiajuosčiu laidiniu ar belaidžiu fiksuotu ryšiu, 42 proc. – mobiliojo ryšio tinklais. 81 proc. internetu besinaudojančių asmenų naudojosi juo kasdien. Lietuvos statistikos departamento duomenimis, 2015 m. kompiuterius ir elektroninius tinklus

18 Lietuvos gyventojų mokėjimo įpročių apklausos apžvalga, Lietuvos bankas, 2015. Žiūrėta 2017 02 11// https://www.lb.lt/lietuvos_gyventoju_mokejimo_iprociu_apklausos_apzvalga_2015_m

19 Ten pat.

prekybai (prekėms ar paslaugoms pirkti arba parduoti) naudojo 36,5 proc. įmonių (2014 m. – 36 proc.). Pavyzdžiui 2016 m. pradžioje interneto svetainę turėjo 75,2 proc. įmonių (2015 m. – 77,3 proc.). Dalis mažų ir vidutinių įmonių savo virtualų turinį perkelia į socialius tinklus ir atsisako interneto svetainių palaikymo išlaidų.

CERT-LT 2016 m. II ketvirčio duomenimis[20], informacinių sistemų užvaldymų (2 290) ir elektroninių duomenų klastojimų (147) skaičius auga ne pirmą ketvirtį: abiejų tipų incidentų buvo kone 80 proc. daugiau, nei prieš metus. Be to, žymiai padaugėjo elektroninių paslaugų trikdymo atvejų – 36. Aptariamojo ketvirčio balandžio ir gegužės mėn. vyko nuolatinės paslaugų trikdymų atakos (DDoS), nukreiptos prieš Lietuvos Respublikos institucijų, žiniasklaidos, bankų ir privačiojo sektoriaus svetaines. Šių atakų metu piktavaliai naudojo įvairius atakų būdus, apsunkindami svetainių administratorių gynybą ir šių atakų valdymą. CERT-LT duomenimis, pastarosios kibernetinės atakos yra sudėtingos ir skiriasi pagal naudojamus atakų metodus.

2.2. Kibernetinio saugumo strategijų / programų Lietuvoje apžvalga

Tokia apžvalga naudinga tam, kad parodyti, kaip kito Lietuvos atitinkami dokumentai bei jų turinys ir kokios probemos buvo vyraujančios atitinkamuose dokumentuose.

Atitinkamos srities strateginio teisinio reguliavimo poreikis Lietuvoje atsirado dar 2001 m., kai Lietuvos Respublikos Vyriausybė 2001 m. gruodžio 22 d. priėmė nutarimą Nr. 1625 „Dėl Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo“ (toliau – 2001 m. strategija), šiuo nutarimu buvo patvirtinta pirmoji nacionalinė informacinių technologijų saugos strategija, tačiau tuo metu „kibernetinio saugumo“ terminas dar nebuvo vartojamas. Svarbiausias šios strategijos tikslas – reglamentuoti tik valstybinių institucijų ir įstaigų saugumą, o informacinių privataus sektoriaus technologijų sauga nebuvo reglamentuojama. Turint omenyje, kad dažniausiai 85–90 proc. kibernetinės infrastruktūros valdoma privataus sektoriaus, ir žiūrint iš dabartinio teisinio reguliavimo pozicijų, galima teigti, kad tuo metu buvo padaryta didelė klaida, nesiekiant reguliuoti privataus sektoriaus IT saugos. Ši teisinio reguliavimo spraga Lietuvoje buvo ištaisyta, tačiau gerokai vėliau

Pirmoji Lietuvos strategija dėl elektroninės informacijos saugos viešajame sektoriuje – Lietuvos elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 m. – galiojo nuo 2006 m. iki 2008 m. Strategijoje naudojamas jau kitoks terminas – „elektroninės informacijos sauga“. Jau iš strategijos pavadinimo aišku, kad Valstybinė strategija skirta išimtinai valstybės institucijų sektoriui – taip susiaurinta informacijos saugos reguliavimo sritis. Ši tendencija jau tuo metu kėlė tam tikrą nerimą, nes informacijos saugumas negali būti veiksmingai užtikrinamas reguliuojant tik valstybės institucijų sektorių ir paliekant nuošalyje privatų sektorių.

Svarbiausi Valstybinės strategijos iškelti tikslai buvo tokie:

- Tobulinti elektroninės informacijos saugos koordinavimą ir priežiūrą. Šiam tikslui pasiekti numatyti tokie uždaviniai: užtikrinti elektroninės informacijos saugos koordinavimą; sukurti efektyvią kovos su nusikalstamomis veikomis, vykdomomis elektroninės informacijos perdavimo aplinkoje, sistemą.
- Teisės aktais reguliuoti elektroninės informacijos saugą. Šiam tikslui pasiekti numatyti tokie uždaviniai: priimti teisės aktus, reguliuojančius elektroninės informacijos saugą; elektroninės informacijos saugą reglamentuoti saugos dokumentais.

20 2016 m. II ketvirčio CERT-LT veiklos ataskaita, CERT-LT, 2016. Žiūrėta 2016 09 28 // https://www.cert.lt/doc/2016_2.pdf

- Kelti elektroninės informacijos saugos kultūrą. Šiam tikslui pasiekti numatyti tokie uždaviniai: valstybės tarnautojus ir darbuotojus, dirbančius pagal darbo sutartis, mokyti elektroninės informacijos saugos; skatinti elektroninės informacijos saugos svarbos suvokimą.
- Tobulinti elektroninės informacijos perdavimo infrastruktūros saugą. Šiam tikslui pasiekti numatytas uždavinys – tobulinti Saugiame valstybiniame duomenų perdavimo tinkle saugomos ir perduodamos elektroninės informacijos saugą.
- Skatinti elektroninės informacijos saugos užtikrinimo projektų įgyvendinimą. Šiam tikslui pasiekti numatytas uždavinys – įgyvendinant elektroninės informacijos saugos projektus, naudotis privataus sektoriaus patirtimi.

Šioje strategijoje, kaip ir 2001 m., buvo paskirtos institucijos, atsakingos už šios strategijos įgyvendinimą. Palyginti su ankstesniąja strategija, institucinis modelis taikomas gerokai plačiau, paskirtos septynios institucijos, atsakingos už 2006 m. strategijoje numatytų priemonių įgyvendinimą, tačiau ir vėl – tik valstybiniame sektoriuje. Be to, nebuvo aiškiai atskirtos institucijų funkcijos, ypač politikos formavimo ir įgyvendinimo kontekste – atsakingosios institucijos buvo nurodytos tik kaip atsakingi priemonių plano vykdytojai. Nebuvo įvardyta ir pagrindinė Lietuvos elektroninės informacijos saugos institucija.

Reikėtų pabrėžti, kad neatsižvelgiant į šioje strategijoje užsibrėžtus tikslus, uždavinių, skirtų šiems tikslams pasiekti, formuluotės buvo tik deklaratyvios, abstrakčios ir nekonkrečios. Daugiau informacijos apie strategijos trūkumus galima rasti moksliniame straipsnyje „Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė“[21]. Minima Valstybinė strategija nustojo galioti 2008 m. ir nuo to laiko Lietuvoje nebuvo jokios galiojančios elektroninės informacijos saugos strategijos ar programos.

Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos patvirtinimo“ buvo patvirtinta Kibernetinio saugumo plėtros programa 2011–2019 m. (toliau – Kibernetinio saugumo programa). Atkreiptinas dėmesys, kad Kibernetinio saugumo programa buvo patvirtinta dar 2011 m., kai Europos Komisija net nebuvo paskelbusi konsultacijos dėl ES kibernetinio saugumo strategijos, todėl ši programa formaliai nebuvo derinama su ES kibernetinio saugumo strategija.

Kibernetinio saugumo programa parengta atsižvelgiant į tai, kad valstybės ir visuomenės gyvenime vis didesnę reikšmę įgyja informacinėmis ir ryšių technologijomis tvarkoma bei perduodama elektroninė informacija, o atsiradusios didesnės elektroninės informacijos tvarkymo galimybės paskatino nacionalinių ir globalių informacinių visuomenių kūrimąsi ir sudarė sąlygas toliau modernizuoti šalių ūkius bei efektyviau valdyti valstybę, tačiau tuo pat metu į elektroninę erdvę perkeliama vis daugiau informacijos, sparčiai automatizuojami įvairūs šalies valdymo ir ūkio veiklos procesai, o globali elektroninė erdvė ir joje teikiamos viešosios paslaugos tapo patraukliu atskirų asmenų, nusikalstamų grupuočių, politinių jėgų ir kitų subjektų taikiniu.

Programos paskirtis – nustatyti elektroninės informacijos saugos (kibernetinio saugumo) plėtros tikslus ir uždavinius, kad būtų užtikrintas elektroninės informacijos ir elektroninėje erdvėje teikiamų paslaugų konfidencialumas, vientisumas ir prieinamumas, elektroninių ryšių tinklų, informacinių sistemų ir ypatingos svarbos informacinės infrastruktūros apsauga nuo incidentų ir kibernetinių atakų, asmens duomenų ir privatumo apsauga, be to, nustatyti uždavinius, kurių įgyvendinimas leistų užtikrinti bendrą elektroninės erdvės ir joje veiklą vykdančių subjektų saugumą.

21 Štitilis D., Paškauskas Ž., „Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė,“ *Jurisprudencija* 2 (92), 2007: 37-45. Žiūrėta 2016 08 15//https://www.mruni.eu/en/mokslo_darbai/jurisprudencija/archyvas/dwn.php?id=267948

Strateginis programos tikslas – plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 m. teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 proc. visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 val., o saugiai elektroninėje erdvėje besijaučiančių Lietuvos gyventojų dalis pasiektų 60 procentų.

Nustatyti šie Kibernetinio saugumo programos įgyvendinimo tikslai:

1. Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas.

Kaip nurodoma programoje, šio tikslo siekiama, nes, išskyrus valstybinį sektorių (Lietuvos Respublikos Vyriausybei atskaitingose įstaigose ir institucijose), nėra sukurta elektroninės informacijos saugos valdymo koordinavimo sistema. Vidaus reikalų ministerijai trūksta įgaliojimų tinkamai vykdyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo kontrolę ir koordinavimą, be to, valdymo ir priežiūros struktūra valstybės ir valstybės institucijų mastu nėra hierarchinė, trūksta Lietuvos viešojo ir privataus sektorių subjektų bendradarbiavimo, tai neleidžia veiksmingai planuoti elektroninės informacijos saugos (kibernetinio saugumo) srities plėtros; informacinių technologijų esami ir nuolat aptinkami nauji pažeidžiamumai, jų laiku nepašalinus, sudaro sąlygas trikdyti informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros objektų funkcionavimą, o šių pažeidžiamumų aptikimo ir šalinimo veiksmingumas didėja centralizuojant šią veiklą. Atitiktis keliamiems elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams užtikrina informacinių išteklių saugos valdymą pagal tarptautinių standartų reikalavimus ir gerosios praktikos pavyzdžius, tačiau Lietuvoje nesuformuota veiksminga atitikties valdymo struktūra; organizacijos informacinės brandos modelis leidžia informacinių išteklių valdytojams geriau suvokti informacinių išteklių saugos poreikį ir veiksmingiau valdyti informacinių išteklių saugą. Įvairios valstybės ir visuomenės veiklos sritys nevienodai priklausomos nuo informacinių išteklių ir paslaugų naudojimo, todėl, siekiant veiksmingai paskirstyti lėšas, būtina telkti pastangas ir informacinius išteklius tose srityse, kur ši priklausomybė didesnė; nusikalstamų veikų elektroninėje erdvėje sparčiai daugėja, o didelio masto incidentai elektroninėje erdvėje gali sukelti nacionalinio masto krizę.

Interneto ir kitų informacinės infrastruktūros paslaugų teikėjų teikiamos paslaugos dažnai neužtikrina paslaugų naudotojų saugos. Ekonominiu sunkmečiu elektroninės informacijos saugai (kibernetiniam saugumui) skiriama nepakankamai dėmesio ir informacinių išteklių, o taikant kolektyvinės saugos principą būtų veiksmingiau naudojami informaciniai ištekliai; nėra sukurtas informacinių išteklių ir infrastruktūros rezervas, skirtas ypatingos svarbos infrastruktūros ir informacinių išteklių veikimui palaikyti kritiniais atvejais. Patikimas tapatybės nustatymas sumažina didelės dalies grėsmių, susijusių su kibernetine erdve, keliamą riziką ir skatina vartotojų pasitikėjimą internetu.

Saugia elektronine erdve (elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimu) yra suinteresuoti visi subjektai, kurių veikla susijusi su elektroninėje erdvėje teikiamomis paslaugomis (valstybės institucijos, privatūs ūkio subjektai, akademinė bendruomenė ir kiti). Bendradarbiaujant vykdomi elektroninės informacijos saugos (kibernetinio saugumo) projektai leidžia užtikrinti visų dalyvaujančių šalių interesų apsaugą.

Elektroninė erdvė yra globali, neturinti nacionalinių ribų, taigi įvairios grėsmės joje plinta labai sparčiai. ES ir *NATO* skiria daug dėmesio e. informacijos ir ypatingos svarbos informacinės infrastruktūros saugai. Kolektyvinės apsaugos principu tikslinga vadovautis ne tik nacionaliniu, bet ir tarptautiniu lygiu. Kompetentingų specialistų bendradarbiavimas, keitimasis turima informacija ir patirtimi yra būtina veiksmingo išankstinio perspėjimo ir prevencinės veiklos sąlyga.

2. *Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą.*

Šio tikslo siekiama, nes ypatingos svarbos informacinės infrastruktūros saugumas užtikrinamas tik žinybiniu lygmeniu, nesuformuota koordinavimo struktūra, neišanalizuoti šios infrastruktūros objektų tarpusavio ryšiai ir sutrikdymo poveikis nacionaliniu mastu, nevykdomas veiklos tęstinumo planavimas. Bandymų įsilaužti būdas (angl. *penetration test*) yra objektyviausias siekiant įsitikinti, ar tinkamai veikia saugos sistema, tačiau jo taikymas nereglamentuotas, tiesiog nėra tokių bandymų praktikos. Veiksminga stebėsenos sistema sudaro sąlygas užtikrinti incidentų prevenciją.

3. *Siekti užtikrinti Lietuvos gyventojų ir šalyje esančių asmenų saugumą elektroninėje erdvėje.*

Šio tikslo siekiama, nes ne visi elektroninės informacijos vartotojai rūpinasi elektroninės informacijos sauga (kibernetiniu saugumu), šiuo metu stinga ir ateityje, tikėtina, vis labiau stigs kvalifikuotų elektroninės informacijos saugos specialistų. Bazinės elektroninės informacijos saugos (kibernetinio saugumo) žinios ir įrankiai leidžia jos vartotojams išvengti daugelio grėsmių elektroninėje erdvėje.

Elektroninės erdvės saugumui užtikrinti būtina nenutrūkstamai veikianti ir tinkamai valdoma sistema, apimanti visą incidentų gyvavimo ciklą: išankstinio perspėjimo, prevencijos, aptikimo, likvidavimo ir tyrimo fazes. Siekiant kovoti su kenksminga programine įranga nuotoliniu būdu valdomų kompiuterių tinklais ar kitais kenkiamosios veiklos elektroninė erdvėje būdais, veiksminga blokuoti interneto prieigą kenkiamąją veiklą vykdantiems asmenims ir (ar) įrenginiams. Šiuo metu visuomenėje yra susiformavęs stereotipas dėl nebaudžiamumo už neteisėtus veiksmus elektroninėje erdvėje, todėl svarbu šį stereotipą kuo greičiau paneigti.

Kibernetinės atakos, kurių šaltinis yra užsienyje, gali ir turi būti stabdomos ties virtualiu Lietuvos elektroninės erdvės perimetru, siekiant išvengti jų poveikio šalies vidaus elektroninių ryšių tinklams. Lietuvos interneto srauto mainų (*ISM*) mazgas yra natūraliai susiformavęs subjektas, į kurį patogu ir veiksminga telkti Lietuvos elektroninės erdvės (ir virtualaus perimetro) apsaugos pajėgumus.

Šiuo metu vyrauja elektroninėje erdvėje teikiamų paslaugų unifikavimo ir centralizavimo tendencija, siekiant įgyvendinti vieno langelio principą; šia tendencija tikslinga naudotis ir užtikrinant šių paslaugų saugą. Vartotojų pasitikėjimas elektroninėje erdvėje teikiamomis paslaugomis yra vienas svarbiausių šių paslaugų populiarumo ir tolesnės plėtros veiksnių.

Kiekvienam tikslui keliami ir atitinkami uždaviniai. Visa tai įmanoma pasiekti tik turint gana gerai parengtų specialistų, kurių įgytas išsilavinimas būtų glaudžiai susijęs su informacinių technologijų ir informacijos saugumo vadyba. Lietuvos Respublikos Vyriausybės nutarime yra pabrėžiama, kad jau šiuo metu yra jaučiamas kvalifikuotų informacijos saugos specialistų trūkumas, ir numatoma, kad ateityje tas trūkumas tik dar labiau didės. Tokių specialistų stygius yra akcentuojamas ir ES dokumentuose, ir nurodant bei aprašant programos tikslus.

Paminėtina, kad kibernetinio saugumo programos vertinimo kriterijai ir jų reikšmės pateikiami šios programos priede. Kibernetinio saugumo programos įgyvendinimą koordinuoja Lietuvos Respublikos vidaus reikalų ministerija, o už šios programos tikslų ir uždavinių įgyvendinimą atsako priede nurodytos įstaigos bei institucijos.

Analizuojant Lietuvos kibernetinio saugumo programą ES kibernetinio saugumo strategijos ir direktyvos bei kitų nagrinėtųjų užsienio valstybių kibernetinio saugumo strategijų kontekste, pabrėžtina, kad programa neužtikrina visapusiškos Lietuvos kibernetinio saugumo strategijos ir kol kas neatitinka visų 2013 m. ES kibernetinio saugumo strategijoje nustatytų kibernetinio saugumo prioritetų bei neužtikrina kitų valstybių kibernetinio saugumo strategijose numatytų kai kurių svarbiausių tikslų ir uždavinių:

1. nenumatytos valstybės ir privataus sektoriaus bendradarbiavimo kibernetinio saugumo srityje priemonės. Turint omenyje, kad šiuo metu dauguma infrastruktūros priklauso privačiam sektoriui, toks bendradarbiavimas yra būtinas;

2. per mažai dėmesio skiriama e. nusikaltimams ir jų kiekiui mažinti. Kaip rodo tyrimai, e. nusikaltimų latentiškumas yra didžiulis. E. nusikaltimai yra kibernetinių atakų pavadinimas baudžiamosios teisės kontekste, todėl šiai nusikaltimų rūšiai programoje turėtų būti skiriamas deramas dėmesys;
3. nenumatyta išsami ir sisteminė kibernetinės gynybos politika. Šiuo metu Lietuvoje nėra nustatyta, kokių veiksmų turėtų būti imamasi kilus kibernetinei grėsmei, kokios yra atskirų „žaidėjų" funkcijos ir atsakomybė, kam teikiami prioritetai saugant kritinę infrastruktūrą nuo kibernetinių atakų, kokie institucijų ir privataus sektoriaus veiksmai kibernetinių atakų atveju. Šį trūkumą būtina kuo skubiau šalinti;
4. neaptariami instituciniai klausimai, nedetalizuojamos atitinkamų institucijų funkcijos ir atsakomybė kibernetinio saugumo srityje;
5. nenumatyti tikslai ir uždaviniai, susiję su visuomenės informavimu ir švietimu, nors tai ir būtina šiuolaikinei informacinei visuomenei, nes kibernetinio saugumo grėsmė dažniausiai susijusi su galutiniais interneto vartotojais;
6. kai kurios užsibrėžtos priemonės yra sunkiai įgyvendinamos arba nepamatuojamos, o tam tikrus indikatorius gali būti sunku įvertinti.

Bendrai pabrėžtina, kad strategijoje iškelti tikslai ir uždaviniai nelabai konkretūs (abstraktūs), ne visais atvejais atspindi elektroninės erdvės keliamus pavojus ir riziką. Tikslams ir uždaviniams pasiekti nėra sukurta kibernetinio saugumo valdymo koordinavimo sistema ir nenumatytas konkrečių lėšų skyrimas.

Nors ir *ENISA*, ir kitos organizacijos savo tinklalapiuose nurodo, kad Lietuva turi patvirtintą kibernetinio saugumo strategiją, vis dėlto kyla klausimas, ar ši programa laikytina visaverte kibernetinio saugumo strategija. Programa neatitinka kompleksinės Lietuvos kibernetinio saugumo vizijos su tipiniais tokios vizijos elementais. Programoje nėra numatytų principų, prioritetų ir kitų elementų. Manytina, kad Lietuvai reikia visaapimančios ir visavertės kibernetinio saugumo strategijos, orientuotos į šiuolaikines grėsmes ir kibernetinio saugumo aktualijas.

2.3. Teisinės aplinkos Lietuvoje apžvalga

Visų pirma, aptartini pagrindiniai ES dokumentai, kurie nulemia Lietuvos teisinę aplinką kibernetinio saugumo srityje.

ES kibernetinio saugumo strategija – bendras strateginės reikšmės ES dokumentas. Strategijoje siūlomi konkretūs veiksmai, kuriais galima padidinti bendrus ES pasiektus rezultatus. Strategijoje pateikta ES vizija yra orientuota į penkis aptartiesiems uždaviniams spręsti skirtus strateginius prioritetus: 1. pasiekti kibernetinį atsparumą, 2. radikaliai sumažinti elektroninių nusikaltimų skaičių, 3. sukurti kibernetinės gynybos politiką ir pajėgumus, susijusius su bendra saugumo ir gynybos politika, 4. plėtoti pramoninius ir technologinius išteklius kibernetiniam saugumui užtikrinti, 5. sukurti nuoseklią tarptautinę Europos Sąjungos elektroninės erdvės politiką ir remti pagrindines ES vertybes[22].

Komisija, Vyriausiasis įgaliotinis ir valstybės narės turėtų suformuluoti nuoseklią ES tarptautinę elektroninės erdvės politiką, kurios tikslas – sustiprinti įsipareigojimų sąsajas ir ryšius su pagrindiniais tarptautiniais partneriais ir organizacijomis, taip pat su pilietine visuomene ir privačiuoju sektoriumi. Strategijoje išdėstoma ES vizija ir būtini veiksmai orientuojantis į tvirtą apsaugą ir paramą piliečių teisėms, kad ES internetinė aplinka taptų saugiausia pasaulyje.

22 ES kibernetinio saugumo strategija. 2013. Prieiga per internetą: http://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52013JC0001&from=LT

Ši strategija nėra teisiškai privalomas dokumentas, tačiau jis formuoja gaires ateities ES kibernetinio saugumo užtikrinimo vystymui ir į šio dokumento nuostatas patartina atsižvelgti.

Europos Parlamento ir Tarybos Direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti[23], nustato pareigą visoms valstybėms narėms priimti nacionalinę tinklų ir informacinių sistemų saugumo strategiją (1 str. 2 a)). Direktyvos 7 straipsnyje yra detalizuojama, kad kiekviena valstybė narė priima nacionalinę tinklų ir informacinių sistemų saugumo strategiją, kurioje visų pirma nagrinėjami šie klausimai:

- nacionalinės tinklų ir informacinių sistemų saugumo strategijos tikslai ir prioritetai;
- valdymo sistema, skirta nacionalinės tinklų ir informacinių sistemų saugumo strategijos tikslams ir prioritetams įgyvendinti, įskaitant valdžios įstaigų ir kitų atitinkamų subjektų vaidmenis ir įsipareigojimus;
- parengties, reagavimo ir atkūrimo priemonių, įskaitant viešojo ir privačiojo sektorių bendradarbiavimą, nustatymas;
- švietimo, informuotumo didinimo ir mokymo programų, susijusių su nacionaline tinklų ir informacinių sistemų saugumo strategija, nurodymas;
- mokslinių tyrimų ir plėtros planų, susijusių su nacionaline tinklų ir informacinių sistemų saugumo strategija, nurodymas;
- rizikos vertinimo planas, skirtas rizikai nustatyti;
- įvairių subjektų, dalyvaujančių įgyvendinant nacionalinę tinklų ir informacinių sistemų saugumo strategiją, sąrašas.

Be to, Direktyvoje yra reglamentuojamas bendradarbiavimo grupės sukūrimas, kad būtų remiamas ir lengvinamas valstybių narių strateginis bendradarbiavimas ir keitimasis informacija, taip pat didinama jų atsakomybė ir tarpusavio pasitikėjimas (11 str.); Reagavimo į kompiuterinius saugumo incidentus tarnybų tinklo (toliau – CSIRT tinklo) sukūrimas, kad būtų prisidedama prie valstybių narių atsakomybės ir tarpusavio pasitikėjimo didinimo ir skatinamas greitas bei veiksmingas operatyvinis bendradarbiavimas (9 str.); nustatomi saugumo ir pranešimo reikalavimai esminių paslaugų operatoriams ir skaitmeninių paslaugų teikėjams (14 str.); nustatomos valstybių narių pareigos paskirti nacionalines kompetentingas institucijas, bendruosius informacinius centrus ir CSIRT, kuriems pavedamos užduotys, susijusios su tinklų ir informacinių sistemų saugumu (15 str).

Kai tos pačios valstybės narės kompetentinga institucija, bendrasis informacinis centras ir CSIRT yra atskiri, jie bendradarbiauja, kad vykdytų Direktyvoje nustatytas pareigas 15 (str.). Ne vėliau kaip 2018 m. lapkričio 9 d. valstybės narės kiekviename iš Direktyvos II priede nurodytų sektorių ir subsektorių identifikuoja esminių paslaugų operatorius, kurie yra įsisteigę jų teritorijoje (5 str.). Direktyvos Baigiamosiose nuostatose yra įtvirtintos valstybių narių nustatomos sankcijos, taikomos pažeidus pagal Direktyvą priimtas nacionalines nuostatas, taisykles ir būtinos priemonės užtikrinti, kad šios sankcijos būtų įgyvendinamos (21 str.).

Įgyvendinant Direktyvą 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti, valstybės narės privalo parengti nacionalinę tinklų ir informacinių sistemų saugumo strategiją, priimti atitinkamus įstatymus bei susijusius teisės aktus. Jeigu yra būtina, valstybės narės gali pasitelkti ENISA, kad pastaroji pagelbėtų joms rengti nacionalinę tinklų ir informacinių sistemų saugumo strategiją bei susijusias priemones[24]. ENISA taip pat atskiroje studijoje dėl nacionalinių

23 Europos Parlamento ir Tarybos Direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. 2016. Prieiga per internetą: .

24 ENISA NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies. 2016. Prieiga per internetą: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

tinklų ir informacinių sistemų saugumo strategijų rengimo, pateikia rekomendacijas valstybėms narėms dėl strategijų rengimo. Direktyva mini 7 kritinės infrastruktūros sektorius, kurie turi būti įtraukiami planuojant ir įgyvendinant kibernetinio saugumo priemones. Tačiau tuo pačiu ENISA rekomenduoja šalims, kurios dar tik pradeda rengti savo nacionalines tinklų ir informacinių sistemų saugumo strategijas, kad pastarosios ypač atsižvelgtų bei nustatytų prioritetus dėl savo valstybės kritinės infrastruktūros sektorių. Nustatant konkrečius sektorius turi būti vadovaujamasi koncentravimosi į kelis sektorius metodu labiau nei „visko padengimo" principu, t.y aprėpiant visus kritinės infrastruktūros sektorius. Tokiu būdu bus pasiektas didesnis progresas ir tuo pačiu bus išgryninami gerieji pavyzdžiai, kurie vėliau galės būti panaudojami ir kituose kritinės infrastruktūros sektoriuose[25]. Rengiant nacionalines tinklų ir informacinių sistemų saugumo strategijas valstybės narės taip pat turėtų vengti neaiškumų, abstraktumų, informacijos dubliavimo apibrėžiant valstybės institucijų funkcijas ir atsakomybes. Viešų ir privačių institucijų atsakomybės kibernetinių incidentų atvejais turėtų būti aiškiai apibrėžiamos[26].

Šią direktyvą Lietuvoje reikės įgyvendinti iki 2018 m. gegužės mėnesio, tad kuriant Lietuvos kibernetinio saugumo strategiją, šios direktyvos nuostatos yra labai svarbios ir į jas reikės atsižvelgti.

Europos Parlamento ir Tarybos Direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR, nustatomos būtiniausios taisyklės, susijusios su nusikalstamų veikų apibrėžtimi, ir sankcijos atakų prieš informacines sistemas srityje (1 str.). Ja taip pat siekiama sudaryti palankesnes sąlygas tokių nusikalstamų veikų prevencijai ir pagerinti teisminių ir kitų kompetentingų institucijų bendradarbiavimą. Šios direktyvos tikslai yra suderinti valstybių narių baudžiamąją teisę atakų prieš informacines sistemas srityje, nustatant būtiniausias taisykles, susijusias su nusikalstamų veikų apibrėžtimi, taip pat atitinkamas sankcijas šioje srityje, ir pagerinti valstybių narių kompetentingų institucijų, įskaitant policiją ir kitas specializuotas teisėsaugos tarnybas, taip pat Sąjungos kompetentingų specializuotų agentūrų ir įstaigų, pavyzdžiui, Eurojusto, Europolo ir Europos kovos su elektroniniais nusikaltimais centro bei Europos tinklų ir informacijos apsaugos agentūros (ENISA), bendradarbiavimą[27]. Ši direktyva Lietuvos nacionalinėje teisėje jau įgyvendinta.

Antra, aptariant Lietuvos teisinę aplinką kibernetinio saugumo srityje, pradėtina nuo pagrindinio Lietuvos Respublikos įstatymo – Lietuvos Respublikos Konstitucijos.

Lietuvos Respublikos Konstitucijos 135 straipsnis nustato, kad Lietuvos Respublika, įgyvendindama užsienio politiką, vadovaujasi visuotinai pripažintais tarptautinės teisės principais ir normomis, siekia užtikrinti šalies saugumą ir nepriklausomybę, piliečių gerovę ir pagrindines jų teises bei laisves, prisideda prie teise ir teisingumu pagrįstos tarptautinės tvarkos kūrimo. Valstybės saugumo garantijos funkcija yra LR Konstitucijos 94 str. yra pavesta Lietuvos Respublikos Vyriausybei. Šio straipsnio 1 dalis nurodo, jog Lietuvos Respublikos Vyriausybė: tvarko krašto reikalus, saugo Lietuvos Respublikos teritorijos neliečiamybę, garantuoja valstybės saugumą ir viešąją tvarką.

25 Ten pat, p. 52.

26 Ten pat, p. 52–53.

27 Europos Parlamento ir Tarybos Direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR. 2013. Prieiga per internetą: http://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32013L0040&from=LT

2012 m. Nacionalinio saugumo strategija galiojo iki 2017 m. sausio 25 d. Ši strategija nustatė gyvybinius ir pirmaeilius nacionalinio saugumo interesus, pagrindinius rizikos veiksnius, pavojus ir grėsmes šiems interesams, pateikia nacionalinio saugumo sistemos plėtros, užsienio, gynybos ir vidaus politikos prioritetus, ilgalaikius ir vidutinio laikotarpio uždavinius. Ši strategija yra grindžiama Lietuvos Respublikos Konstitucija, Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymu (toliau – Nacionalinio saugumo pagrindų įstatymas), Šiaurės Atlanto ir Europos Sąjungos sutartimis (1 p.). Formuodama ir įgyvendindama nacionalinio saugumo politiką, Lietuvos Respublika laikosi visuotinai pripažintų tarptautinės teisės normų, principų ir įsipareigojimų, įtvirtintų Jungtinių Tautų Organizacijos (toliau – JTO), Europos saugumo ir bendradarbiavimo organizacijos (toliau – ESBO) ir Europos Tarybos dokumentuose, prisideda prie tarptautinės taikos ir visaapimančio saugumo, pagrįsto demokratinėmis vertybėmis, teise ir teisingumu, palaikymo (3 p.). Gyvybiniai nacionalinio saugumo interesai – interesai, kuriems apsaugoti naudojamos visos teisėtos priemonės ir kuriuos pažeidus kiltų rimta grėsmė Lietuvos valstybės ir visuomenės egzistavimui (7 p.). Tokie interesai apima suverenitetą, pilietinę visuomenę, taiką ir kt.

Pirmaeiliai nacionalinio saugumo interesai strategijoje buvo apibūdinami kaip interesai, kurių neginant laikui bėgant būtų pažeidžiami gyvybiniai Lietuvos Respublikos interesai. Tarp pirmaeilių nacionalinio saugumo interesų Lietuvoje minimas ir kibernetinis saugumas.

Strategijoje buvo apibūdinami rizikos veiksniai, pavojai ir grėsmės nacionaliniam saugumui (IV skyrius); nacionalinio saugumo politikos įgyvendinimo prioritetai ir uždaviniai (V skyrius). Kibernetinės atakos priskiriamos prie išorinių veiksnių. Strategijoje pateikiama „kibernetinių atakų“ sąvoka: „*elektroninių ryšių tinklų ir informacinių sistemų atakos, kuriomis siekiama sutrikdyti nacionaliniam saugumui strategiškai svarbių ūkio sektorių infrastruktūros funkcionavimą ir nacionaliniam saugumui svarbių valstybės institucijų veiklą, išgauti įslaptintą informaciją, vykdyti kitas nusikalstamas veikas ir taip pakenkti valstybės ir jos piliečių saugumui*.“ Taip pat, prie išorinių veiksnių minimas tarptautinis organizuotas nusikalstamumas ir kiti tarpvalstybiniai nusikaltimai, į kurio apibrėžimą įeina ir nusikaltimai elektroninėje erdvėje.

Užsienio politikos srityje, nacionalinio saugumo kontekste, buvo numatyti tokie planai: „prisidės prie kolektyvinės gynybos pajėgumų stiprinimo, rems NATO valstybių narių apginamumo planų rengimą ir atnaujinimą, sieks NATO matomumo ir karinio buvimo Lietuvoje didinimo, NATO branduolinės politikos stabilumo, sudarys sąlygas NATO mokymams ir pratyboms, prisidės prie NATO pajėgumų, skirtų naujo pobūdžio (energetinio, kibernetinio, informacinio saugumo) grėsmėms atremti, plėtojimo ir išmaniosios gynybos projektų.“

Stiprinant gynybos pajėgumus, turėtų būti plėtojamas kariuomenės atsakas į nekonvencinius saugumo iššūkius (energetinio, kibernetinio, informacinio saugumo).

Užtikrinant energetinį saugumą, pagal Strategiją, turėtų būti užtikrinamas svarbiausių energetikos sektoriaus įmonių patikimas veikimas, fizinis ir kibernetinis saugumas <...>.

Strategijoje buvo aptariamas elektroninės informacijos saugos (kibernetinio saugumo) stiprinimas: „Siekdama visapusiškai stiprinti nacionalinės elektroninės erdvės saugumą, užtikrinti elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą, Lietuvos Respublika:

- kurs nacionalinę koordinavimo sistemą kibernetinio saugumo srityje, tobulins nacionalinį elektroninės informacijos saugos (kibernetinio saugumo) srities teisinį reglamentavimą ir dalyvaus tarptautinėse teisinio reglamentavimo tobulinimo iniciatyvose;
- stiprins nacionalinius gebėjimus reaguoti į elektroninės informacijos saugos incidentus (įskaitant kibernetines atakas) nacionalinėje elektroninėje erdvėje ir likviduoti jų padarinius;

– sieks užtikrinti nacionaliniam saugumui strategiškai svarbios informacinės infrastruktūros saugą;
– stiprins elektroninės informacijos saugos (kibernetinio saugumo) kultūrą plėtodama bendradarbiavimą tarp viešojo, privataus, nevyriausybinio ir mokslo sektorių bei su tarptautiniais partneriais.“

Baigiamosiose nuostatose buvo nurodoma, kad Lietuvos Respublika, atsižvelgdama į tai, kad išorės ir vidaus saugumo aplinka gali keistis sukeldama naujus rizikos veiksnius, pavojus ir grėsmes nacionaliniam saugumui, turi būti tinkamai pasirengusi į juos atsakyti ir apsaugoti savo nacionalinius interesus (17).

Atsižvelgiant į tai, kad ši strategija buvo priimta dar 2012 m., 2016 m. yra parengtas atnaujintos **nacionalinio saugumo strategijos projektas**, kuris buvo užregistruotas Seime[28]. 2017 m. sausio 17 d. šis projektas buvo priimtas. Naujoji nacionalinio saugumo strategijos redakcija įsigaliojo 2017 m. sausio 26 d.[29] Ši naujoji Strategija nustato gyvybinius ir pirmaeilius nacionalinio saugumo interesus, pagrindinius rizikos veiksnius, pavojus ir grėsmes šiems interesams, nacionalinio saugumo sistemos plėtros, užsienio, gynybos ir vidaus politikos prioritetus, ilgojo ir vidutinio laikotarpių uždavinius (1 p.). Nacionalinis saugumas strategijos projekte suvokiamas kaip nacionalinio saugumo interesų apsauga (5 p.).

Strategijoje minima, kad Lietuvos Respublikos saugumo aplinką ypač neigiamai veikia Rusijos Federacijos veiksmai, pažeidžiantys tarptautines normas ir griaunantys taisyklėmis pagrįstą saugumo architektūrą Europoje (8 p.). Lietuvos Respublikos saugumas tiesiogiai ir netiesiogiai priklauso nuo ilgalaikių saugumo iššūkių Europos Pietų kaimynystės valstybėse (9 p.). Pagal Strategiją, „Atsižvelgiant į pakitusią saugumo aplinką, konvencinės karinės grėsmės Lietuvos Respublikai ar kitai regiono šaliai nebėra teorinės, o karinės ir nekarinės (diplomatinės, informacinės, kibernetinės, ekonominės, energetinės, finansinės, teisinės) priemonės, nukreiptos prieš Lietuvos Respublikos nacionalinį saugumą, gali būti naudojamos išvien, siekiant paveikti labiausiai pažeidžiamas valstybės gyvenimo sritis.“

Kibernetinės grėsmės apibrėžiamos taip: „veiksmai kibernetinėje erdvėje, kuriais siekiama sutrikdyti ypatingos svarbos informacinių infrastruktūrų funkcionavimą, nacionaliniam saugumui svarbių valstybės institucijų ir ūkio sektorių veiklą, išgauti valstybės ir tarnybos paslaptį sudarančią ar kitą neviešą informaciją, įvykdyti kitas nusikalstamas veikas ir taip pakenkti valstybės ir jos piliečių saugumui.“ **Atkreiptinas dėmesys**, kad formuojant sąvokas, turi būti laikomasi juridinės technikos. Kablelis Lietuvių kalbos gramatikoje ir logikoje reiškia junginį. Taigi, pagal dabartinį apibrėžimą, traktuotina, kad kibernetinei grėsmei konstatuoti, turi būti išpildomos visos sąlygos. Tokiu atveju kibernetinės grėsmės apibrėžimo sąlygų greičiausiai netenkins joks kibernetinis incidentas. Dėl tokios ydingos praktikos gali kilti neigiamos pasekmės, tokios praktikos reikėtų vengti ir formuojant sąvokas strategijose, skirti didelį dėmesį juridinei technikai.

NATO kolektyvinės gynybos stiprinimo srityje Lietuva „dalyvaus stiprinant NATO pasirengimą atsakyti į hibridines grėsmes, taip pat prisidės prie NATO pajėgumų saugumo iššūkiams energetinio, kibernetinio, informacinio saugumo srityse atremti plėtojimo“.

Strategijoje numatytas kibernetinio saugumo stiprinimas: Siekdama visapusiškai stiprinti nacionalinės elektroninės erdvės saugumą, Lietuvos Respublika:

– plėtos nacionalinę kibernetinio saugumo sistemą, ypatingą dėmesį skirdama kibernetinio saugumo reikalavimų įgyvendinimui ir ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių kibernetinio saugumo užtikrinimui;

28 Nutarimo dėl LR Seimo 2002 m. gegužės 28 d. nutarimo Nr. IX-907 „Dėl nacionalinio saugumo strategijos patvirtinimo“ pakeitimo projektas, LR Seimas, 2016. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/407015b094f311e68adcda1bb2f432d1?jfwid=-wd7z8nw39

29 Nutarimas dėl LR Seimo 2002 m. gegužės 28 d. nutarimo Nr. IX-907 „Dėl nacionalinio saugumo strategijos patvirtinimo“ pakeitimo, LR Seimas, 2016. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/2c6e04b0e30811e68503b67e3b82e8bd

- stiprins nacionalinius gebėjimus nustatyti kibernetinio saugumo incidentus, reaguoti į juos ir likviduoti sukeltus padarinius;
- rems NATO, ES, taip pat regioninių kibernetinio saugumo pajėgumų ir incidentų valdymo koordinavimo plėtrą;
- stiprins kibernetinio saugumo kultūrą plėtodama viešojo, privataus, nevyriausybinio ir mokslo sektorių bendradarbiavimą ir su tarptautiniais partneriais;
- stiprins visuomenės švietimą kibernetinio saugumo klausimais.

Baigiamosiose nuostatose numatoma, kad Lietuvos Respublika, atsižvelgdama į tai, kad saugumo aplinka gali keistis sukeldama naujų rizikos veiksnių, pavojų ir grėsmių nacionaliniam saugumui, turi būti tinkamai pasirengusi į juos atsakyti ir apsaugoti savo nacionalinius interesus (19 p.). Pagal Strategijos 20 p., Strategijoje nustatyti ilgojo ir vidutinio laikotarpių nacionalinio saugumo politikos prioritetai ir uždaviniai, tačiau ji turi būti atnaujinama pasikeitus saugumo aplinkai.

2015 m. kovo 18 d. Lietuvos Respublikos Vyriausybė patvirtino **Valstybinę vartotojų teisių apsaugos 2015–2018 metų strategiją**. Vienas iš pagrindinių šios strategijos tikslų – gerinti vartotojų ir verslininkų švietimą ir didinti vartotojų asociacijų vaidmenį. Pagal tai susijęs uždavinys – tobulinti vartotojų ir verslininkų kompetenciją ir didinti pasitikėjimą elektronine erdve (pažangos įgyvendinant šį uždavinį vertinimo kriterijus – vartotojams ir verslo subjektams suteiktų rekomendacijų, konsultacijų ir (ar) metodinės pagalbos paslaugų kibernetinio saugumo klausimais (skleidžiant informaciją per tokias žiniasklaidos priemones ir interneto svetaines kaip www.cert.lt, ir www.esaugumas.lt) skaičius).

1996 m. LR Nacionalinio saugumo pagrindų įstatymas nustato Lietuvos nacionalinio saugumo užtikrinimo pagrindus. Seimas, Respublikos Prezidentas, Vyriausybė ir kitos valstybės institucijos plėtoja Lietuvos nacionalinio saugumo sistemą vadovaudamiesi šio įstatymo nustatytais Nacionalinio saugumo pagrindais. Nacionalinio saugumo strategijai įgyvendinti rengiamos ilgalaikės valstybinės saugumo stiprinimo programos, kurias teikia Vyriausybė ir nutarimu tvirtina Seimas.

Nacionalinio saugumo politikos tikslas – sutelktomis valstybės ir piliečių pastangomis plėtoti ir stiprinti demokratiją, užtikrinti Tautos saugų būvį ir valstybės vidaus bei išorės saugumą, atgrasyti kiekvieną potencialų užpuoliką, ginti Lietuvos valstybės nepriklausomybę, teritorijos vientisumą ir konstitucinę santvarką (Lietuvos nacionalinio saugumo pagrindų įstatymo priedėlio 1 dalies 1 skyrius). Lietuvos gynybinė galia grindžiama: tautos apsisprendimu ir pasiryžimu priešintis kiekvienam užpuolikui; NATO sąjungininkų teikiama pagalba ir solidarumu; įstatymo nustatyta visuotine privalomąja karo tarnyba; kariuomenės ir jos aktyviojo rezervo parengtimi ir apginklavimu; piliečių pasirengimu visuotiniam ginkluotam ir neginkluotam pasipriešinimui bei pilietinei gynybai; geru kariuomenės ir civilių piliečių savitarpio supratimu ir bendradarbiavimu; valstybės atsargomis ir kitais mobilizacinio rezervo ištekliais; šalies mokslo ir studijų institucijų bei įmonių potencialo panaudojimu (Lietuvos nacionalinio saugumo pagrindų 2 skirsnis).

Pagal įstatymo 2 str. (nacionalinio saugumo užtikrinimo subjektai), „Lietuvos nacionalinį saugumą užtikrina Lietuvos Respublikos piliečiai, jų bendrijos ir organizacijos, Respublikos Prezidentas, Seimas, Vyriausybė, kariuomenė, policija, Valstybės saugumo departamentas, kitos šiam tikslui valstybės įsteigtos institucijos, vadovaudamiesi Konstitucija ir įstatymais bei vykdydami savo pareigas ir funkcijas nacionalinio saugumo sistemoje.“ Atkreiptinas dėmesys, kad tarp subjektų įvardijami ir piliečiai.

Įstatymo 5 str. 3 d. nustatyta, kad „ilgalaikės valstybinės saugumo stiprinimo programos įgyvendinamos per strateginio planavimo dokumentus. Programų įgyvendinimą koordinuoja Vyriausybė“. Toks strateginio planavimo dokumentas turėtų būti priimamas ir planavimo kibernetinio saugumo srityje atveju. To paties straipsnio 4 d. nustato finansavimo aspektus: „Vyriausybė, pateikdama ilgalaikes valstybines sau-

gumo stiprinimo programas, kartu pateikia informaciją apie lėšų poreikį, reikalingą kiekvienai programai įgyvendinti. Vyriausybė lėšas programoms įgyvendinti numato rengdama Lietuvos Respublikos atitinkamų metų valstybės biudžeto ir savivaldybių biudžetų finansinių rodiklių patvirtinimo įstatymo projektą. Programoms įgyvendinti taip pat gali būti naudojamos ir kitos teisėtai gautos lėšos.“

Įstatymo priedėlio 2-ojo skyriaus 1-jame skirsnyje yra nustatyti nacionalinio saugumo objektai. Pagrindiniai nacionalinio saugumo objektai yra:

- žmogaus ir piliečio teisės, laisvės bei asmens saugumas;
- tautos puoselėjamos vertybės, jos teisės ir laisvos raidos sąlygos;
- valstybės nepriklausomybė;
- konstitucinė santvarka;
- valstybės teritorijos vientisumas;
- aplinka ir kultūros paveldas;
- visuomenės sveikata.

Elektroninėje erdvėje, kibernetinio incidento atveju, gali būti pažeisti visi šie objektai.

Įstatymo priedėlio 7-ajame skyriuje numatytos svarbiausios Lietuvos gynybos politikos nuostatos. Pirmajame skirsnyje apibūdinamas visuotinės ir besąlyginės gynybos principas, kurio taikymas labai svarbus ir elektroninėje erdvėje. Šis principas numato:

- Lietuvos gynimas yra visuotinis ir besąlyginis, taip pat derinamas su NATO kolektyvinės gynybos principų įgyvendinimu.
- Gynybos visuotinumas reiškia, kad Lietuvą ginklu gina valstybės ir NATO sąjungininkų ginkluotosios pajėgos, kad gynybai panaudojami valstybės ištekliai, kad kiekvienas pilietis ir Tauta priešinasi visais pagal tarptautinę teisę leistinais būdais.
- Gynybos besąlyginumas reiškia, kad Lietuvos gynyba nėra saistoma jokių sąlygų ir kad niekas negali varžyti Tautos ir kiekvieno piliečio teisės priešintis agresoriui, okupantui ir bet kam, kas prievarta kėsinasi į Lietuvos valstybės nepriklausomybę, teritorijos vientisumą ir konstitucinę santvarką. Siekdama NATO sąjungininkų ir kitokios tarptautinės pagalbos gynybai, Lietuva ginasi ir priešinasi pati, nelaukdama, kada toji pagalba bus suteikta.

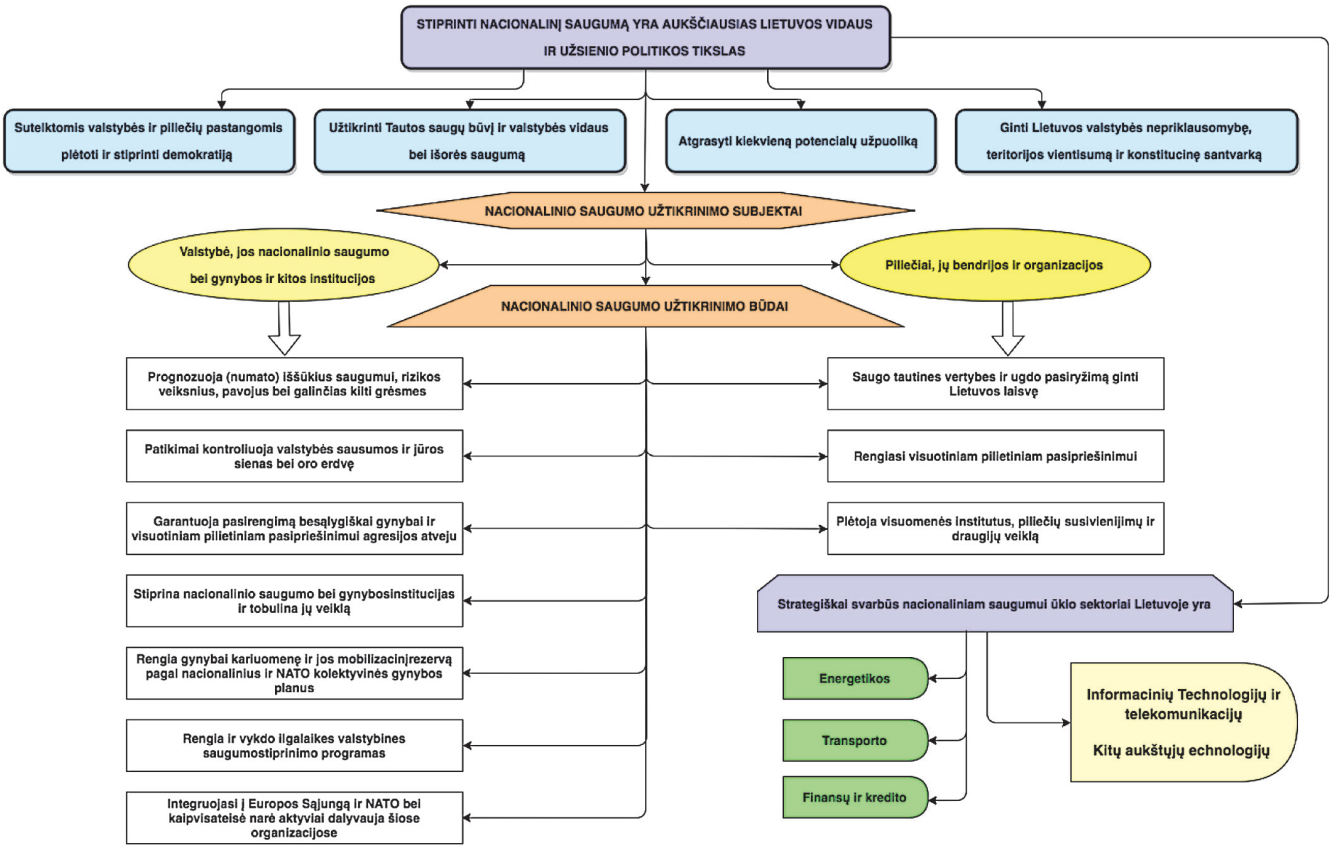
Įstatymo priedėlio 7-ojo skyriaus 2-jame skirsnyje „Bendrosios Lietuvos gynybos nuostatos“ nustatyta, kad „Lietuvos gynybinė galia grindžiama:

- Tautos apsisprendimu ir pasiryžimu priešintis kiekvienam užpuolikui;
- NATO sąjungininkų teikiama pagalba ir solidarumu;
- įstatymo nustatyta visuotine privalomąja karo tarnyba;
- kariuomenės ir jos aktyviojo rezervo parengtimi ir apginklavimu;
- piliečių pasirengimu visuotiniam ginkluotam ir neginkluotam pasipriešinimui bei pilietinei gynybai;
- geru kariuomenės ir civilių piliečių savitarpio supratimu ir bendradarbiavimu;
- valstybės atsargomis ir kitais mobilizacinio rezervo ištekliais.
- šalies mokslo ir studijų institucijų bei įmonių potencialo panaudojimu.“

Panašiais principais Lietuvos gynybinė galia turėtų būti grindžiama ir elektroninėje erdvėje.

Aukščiau paminėtus aspektus galima vizualizuoti taip:

Paveikslėlis Nr. 6. *Autorių sudaryti Nacionalinio saugumo įstatyme apibūdinami svarbiausi aspektai*



Taigi, piliečiams ir bendrijoms tenka pareiga plėtoti visuomenines institucijas ir susivienijimus. Piliečiai ir organizacijos turi rengtis visuotiniam pasipriešinimui. Tenka pastebėti, kad pačiai valstybei atitinkamos pareigos nenustatytos, pati valstybė neprisiima su tuo susijusių pareigų. Tai sukelia pareigų disbalansą šiais aspektais: valstybė turėtų nurodyti kryptis, kaip turėtų kuriamos visuomeninės institucijos ar susivienijimai, arba kaip turėtų būti rengiamasi visuotiniam pasipriešinimui. Taip pat, valstybė turėtų prisidėti prie atitinkamų procesų, kaip partneris.

Atitinkamai, kibernetinio saugumo atveju, turėtų būti taikomas ekvivalentiškumo principas, t.y. kas traktuojama fizinėje erdvėje, neturėtų skirtis ir elektroninėje erdvėje. Taigi, piliečiams turėtų kilti pareigos taip pat prisidėti prie kibernetinio saugumo, kaip nacionalinio saugumo klausimo. O valstybė turėtų savo ištekliais padėti piliečiams ir organizacijoms pasirengti kibernetinei gynybai. Tokia pagalba pasirengime turėtų būti daugiausia suprantama kaip švietimas, kvalifikacijos kėlimas, mokymai ir pan. Taigi, valstybė turėtų skatinti ir inicijuoti savo piliečių kibernetinės higienos laikymąsi ir užtikrinimą.

2015 m. Kibernetinio saugumo įstatymas nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžia kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas, valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones (1 str. 1 d.). Kibernetinis saugumas grindžiamas ben-

draisiais teisės principais, elektroninių ryšių veiklos reguliavimo principais ir šiais kibernetinio saugumo principais: elektroninės erdvės nediskriminavimo; kibernetinio saugumo proporcingumo; viešojo intereso viršenybės (3 str.). Kibernetinio saugumo politikos strateginius tikslus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė (toliau – Vyriausybė). Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija (toliau – Krašto apsaugos ministerija). Lietuvos Respublikos vidaus reikalų ministerija (toliau – Vidaus reikalų ministerija), Nacionalinis kibernetinio saugumo centras, Lietuvos Respublikos ryšių reguliavimo tarnyba (toliau – Ryšių reguliavimo tarnyba), Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Policijos departamentas) formuojant kibernetinio saugumo politiką dalyvauja tiek, kiek šiame įstatyme nustatytoms funkcijoms atlikti reikia nustatyti viešojo administravimo subjektų, valdančių valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų veiklos teisinį reguliavimą (4 str.). Kibernetinio saugumo politiką pagal kompetenciją įgyvendina Vidaus reikalų ministerija, Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas (4 str.). Įstatymas detaliai reglamentuoja kiekvienos iš institucijų įgaliojimus.

Atkreiptinas dėmesys, kad Kibernetinio saugumo įstatyme numatytas kibernetinio saugumo informacinis tinklas, skirtas saugiai keistis informacija tarp kibernetinio saugumo dalyvių:

„17 straipsnis. Kibernetinio saugumo informacinis tinklas

1. Kibernetinio saugumo informacinis tinklas, kurio valdytojas – Nacionalinis kibernetinio saugumo centras, yra saugi informacijos mainų platforma, kurios paskirtis yra dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir bendradarbiavimą tarp kibernetinio saugumo informacinio tinklo narių kibernetinio saugumo srityje.

2. Kibernetinio saugumo informaciniu tinklu gali naudotis tik tie subjektai, kurie atitinka Kibernetinio saugumo informacinio tinklo nuostatuose nurodytus reikalavimus.

3. Kibernetinio saugumo informaciniame tinkle skelbiama aktuali viešojo administravimo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų ir ypatingos svarbos informacinės infrastruktūros valdytojų paskirtų asmenų ar padalinių, atsakingų už kibernetinio saugumo organizavimą ir kibernetinių incidentų valdymą, kontaktinė informacija.“

Tai gali būti vertinama kaip informacijos keitimosi mechanizmas[30].

Šalia įstatymų, reglamentuojančių Lietuvos kibernetinio saugumo aplinką, turėtų būti paminėtas ir **Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo projektas**[31]. Projektu siūloma nustatyti, kad tam tikros debesijos paslaugos būtų priskirtinos valstybei ir jos institucijoms. Projektu taip pat siūloma nustatyti debesijos paslaugų vertinimo tvarką, institucijoms skirtoms debesijos paslaugoms teikti naudojamos techninės ir programinės įrangos suderinamumą, licencijavimą, sertifikavimą, kokybės ir patikimumo reikalavimus.

30 Nors įstatyme ir nustatytas, šis mechanizmas kol kas neveikia praktikoje.

31 Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo projektas, LR Seimas, 2016. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/d0515db0afba11e68987e8320e9a5185?jfwid=-wd7z8bvie

Prie nacionalinės teisinės atlinkos priskirtinas ir 2011 m. LR Vyriausybės nutarimas dėl elektoninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos patvirtinimo. Šis nutarimas, kurio nuostatos detaliau aptartos aukščiau šiame modelyje, nustato elektroninės informacijos saugos (kibernetinio saugumo) plėtros tikslus ir uždavinius, kad būtų užtikrintas elektroninės informacijos ir elektroninėje erdvėje teikiamų paslaugų konfidencialumas, vientisumas ir prieinamumas, elektroninių ryšių tinklų, informacinių sistemų ir ypatingos svarbos informacinės infrastruktūros apsauga nuo incidentų ir kibernetinių atakų, asmens duomenų ir privatumo apsauga, taip pat nustatyti uždavinius, kurių įgyvendinimas leistų užtikrinti bendrą elektroninės erdvės ir joje veiklą vykdančių subjektų saugumą. Programos strateginis tikslas – plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 valandos, o Lietuvos gyventojų, kurie saugiai jaučiasi elektroninėje erdvėje, dalis pasiektų 60 procentų. Programos įgyvendinimą koordinuoja Vidaus reikalų ministerija. Už Programos tikslų ir uždavinių įgyvendinimą atsako institucijos ir įstaigos, nurodytos Programos priede (Krašto apsaugos ministerija, Vidaus reikalų ministerija, Valstybinė asmens duomenų apsaugos inspekcija ir kt.).

Šiame modelyje, sudarant tikslus, prioritetus ir pan., taip pat remiamasi ir Europos Tarybos 2016 m. pateikia Lietuvos kibernetinio saugumo situacijos analize: Septintasis tarpusavio vertinimo etapas „Europos kibernetinių nusikaltimų prevencijos ir kovos su tokiais nusikaltimais politikos praktinis įgyvendinimas ir veikimas“. Įvertinimo ataskaita – Ataskaita apie Lietuvą[32]. Šioje analizėje yra pateikiami tiek teisiniai, tiek veiklos, tiek kiti aspektai apie Lietuvą. Šios analizės tam tikros dalys ir / ar jų atskira turinio informacija nėra kartojamos šiame Modelyje.

32 Įvertinimo ataskaita apie Lietuvą. Septintasis tarpusavio vertinimo etapas „Europos kibernetinių nusikaltimų prevencijos ir kovos su tokiais nusikaltimais politikos praktinis įgyvendinimas ir veikimas“. ES Taryba. Briuselis, 2016. Žiūrėta 2016 11 10 // http://data.consilium.europa.eu/doc/document/ST-6520-2016-REV-1-DCL-1/lt/pdf

3. PRINCIPAI

Kibernetinio saugumo problema apima daug žmogaus veiklos sričių ir kyla iš technologinio pokyčio, t.y. technologijos įgalino sukelti aptariamas saugumo problemas, tačiau ne technologijos sukelia problemas, o žmonės, pasitelkdami technologines galimybes ir pritaikydami savo tikslams siekti, t.y. didžioji dalis problemų yra ne technologinio pobūdžio, o žmogaus santykio su technologijomis bei žmonių santykių su kitais žmonėmis (pvz.: sistemas tikslingai sutrikdo ne pačios technologijos, tiesa, atsitiktiniai sutrikimai įvyksta ir dėl technologijų netobulumo, bet žmonės, siekdami savanaudiškų tikslų (pinigų, valdžios, įtakos ir kt.)), t.y. didelė dalis klausimų yra socialiniai ir juos tiria socialiniai mokslai, todėl jiems spręsti taikytini socialinių mokslų principai, tai gali būti teisės, valdymo, ekonomikos ir kiti principai.

Europos Sąjungos Kibernetinio saugumo strategija išskiria penkis principus:

1. Kas taikoma fizinėje, tas ir elektroninėje erdvėje,
2. Fundamentinių teisių apsauga,
3. Prieiga visiems,
4. Įvairių žaidėjų valdymas,
5. Bendra atsakomybė.

Aptariant šiuos principus svarbu išskirti specifiškiausius, svarbiausius principus bei abejotinus principus. Pradedant nuo abejotinų, reikėtų išskirti bendro pobūdžio visuotinai galiojančius ir kituose svarbiuose dokumentuose įtvirtintus principus, pvz.: „Fundamentinių teisių apsauga“. Ką naujo lemia šio principo išskyrimas kaip specifinio arba bendrojo kibernetinio saugumo principo? Ar nesant Europos Sąjungos Kibernetinio saugumo strategijos šis principas negaliotų arba galiotų siauriau? Šio principo turinys yra pakankamai aiškus ir gerai detalizuotas atitinkamuose tarptautiniuose norminiuose aktuose, pertikrintas autoritetingų tarptautinių teismų ir jo pateikimas šioje strategijoje nėra būtinas, nors ir galimas parodant, kad tai gairė, kuri labai svarbi sprendžiant šios saugumo rūšies pažeidimus, t.y., kad negalima aukoti fundamentinių žmogaus teisių dėl saugumo sprendimų. Kitas abejotinas kibernetinio saugumo principas yra „Prieiga visiems“. Vargu, ar šis principas didina saugumą, greičiau mažina, tiesa, jis svarbus kitu aspektu, t.y. sukurti laisvą ir demokratišką elektroninės erdvės bendruomenę, tačiau neretai tai ir sąlygoja šios elektroninės erdvės pažeidžiamumą.

Specifiniu principu neabejotinai galima išskirti „Kas taikoma fizinėje, tas ir elektroninėje erdvėje“. Šis arba jam labai artimi principai vienaip ar kitaip nurodomi ir kituose norminiuose aktuose reguliuojančiuose elektroninę erdvę, pvz.: elektroninės formos nediskriminavimo ir kt. Kitas tikrai specifinis principas, kaip galima pasiekti kibernetinio saugumo yra „Įvairių žaidėjų valdymas“, nes kibernetinio saugumo galima siekti ir kitokiais principais, pvz.: atitinkamų resursų centralizavimo, kontrolės ar ribojimo, tačiau konkrečioje strategijoje pasisakoma, kad kibernetines grėsmes galima valdyti per įvairius žaidėjus.

Kaip minėta, dalies principų būtų galima ir neminėti, tačiau visų svarbių principų pateikimas vienoje vietoje turi vertę vien todėl, kad visi principai taikytini tik sistemoje ir principų išskyrimas ir surašymas viename dokumente leidžia aiškiau įsivertinti principų visumą ir sistemą.

NATO išskiria tris principus:

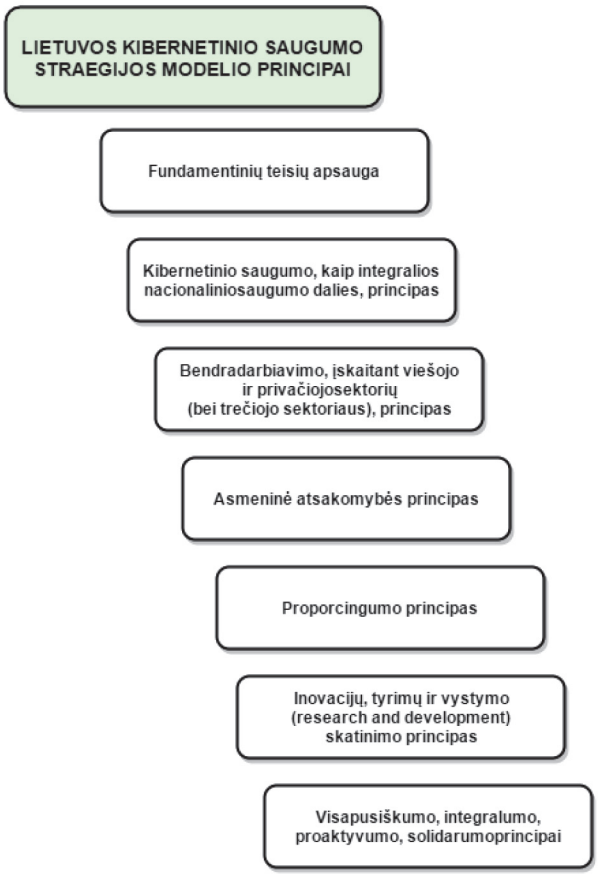
1. Prevencija (Prevention);
2. Atsistatymo (Resilence);
3. Nekartojimo (Non-dublication).

Tai gerokai trumpesnis sąrašas už kitų šalių principų sąrašus, tačiau šiuos principus galima išskirti kaip specifinius kibernetinio saugumo principus.

Skirtingų valstybių kibernetinio saugumo strategijoms yra būdingi panašūs dokumento struktūros elementai, pvz.: nustatomi siektini tikslai, principai ir kt. Strategijose įvardinami skirtingi socialinių mokslų (valdymo, teisės, politikos, ekonomikos, karybos ir kt.) principai. Dalyje strategijų iškelti principai kelia abejonių, ar tai tikrai principai, o gal tik tikslo siekimo būdai arba metodai. Ne visose strategijose išskiriami konkretūs principai, tačiau yra strategijų, kurios išskiria net keliolika principų. Tai rodo ne tik skirtingą kibernetinio saugumo siekimo būdų įvairovę, bet ir valstybių skirtingą suvokimą, kas ir kaip turi būti atspindima strategijose. Reikia atkreipti dėmesį, kad net ir unifikaciją skatinančios ES direktyvos nenumato poreikio nacionalinėse kibernetinio saugumo strategijose numatyti kibernetinio saugumo užtikrinimo principus. Nustatant principus strategijoje tikslinga nustatyti specialius kibernetinio saugumo strategijų principus arba principus, kurie kibernetinio saugumo kontekste įgyja didesnę svarbą negu kitose žmogaus veiklos srityse. Tačiau svarbu, kad į strategiją įrašyti bendrieji ar specialieji principai būtų tikrai kertiniai kibernetinio saugumo pasiekimui, tuomet juos įsivardinus viename dokumente turime nuoseklią principų sistemą, nes principai teisingai taikomi tik vieningoje sistemoje, o vieno ar kito principo suabsoliutinimas ar sureikšminimas gali padaryti žalos visai sistemai ir ją iškreipti.

Lietuvos kibernetinio saugumo strategijos modelyje rekomenduotina nurodyti šiuos **principus**:

Paveikslėlis Nr. 7. *Autorių sudaryti Lietuvos kibernetinio saugumo Strategijos modelio principai*



– **Fundamentinių teisių apsauga** (teisės viršenybė, subsidiarumas, savireguliacija, asmens duomenų apsauga ir kt.).

Kibernetinis saugumas yra tik viena iš priemonių užtikrinti fundamentines žmogaus teises, todėl ši saugumo sritis negali tapti svarbesne už pačias žmogaus teises. Taikant principus būtinas jų sisteminis taikymas, todėl, taikant specifinius kibernetinio saugumo principus, būtina nuolat atsižvelgti į fundamentines žmogaus teises, privatumo ir susižinojimo apsaugos ir kitų principų svarbą.

Išskirtinos dvi šio fundamentinių teisių apsaugos principo dimensijos:

1. Kibernetinio saugumo užtikrinimo vienas iš tikslų – pagrindinių žmogaus teisių ir laisvių apsauga. Kibernetinio saugumo kontekste galima paminėti teisę į privatumą ir išsireiškimo laisvę (atitinkamai, Žmogaus teisių ir pagrindinių laisvių konvencijos 8-asis ir 10-asis straipsniai). Kibernetiniai incidentai tiek gali lemti asmeninės informacijos atskleidimą, tiek sutrikdyti sistemų darbą arba elektroninių ryšių paslaugų teikimą, o tai gali turėti neigiamos įtakos išsireiškimo laisvei.
2. Užtikrinant kibernetinį saugumą, gali būti taikomos saugumo priemonės, pvz., prieblogos ir / ar elektroninių ryšių paslaugų nutraukimas ar ribojimas. Tai gali paveikti asmenų teisę į internetą, kuri kai kuriuose tarptautiniuose neprivalomuose dokumentuoja jau įvardijama kaip viena iš pagrindinių žmogaus teisių. Taip pat, kovojant su kibernetiniais incidentais, elektroniniais nusikaltimais, vykdant prevenciją, gali būti perimamas elektroninių ryšių turinys ar srautas. Tai gali paveikti asmenų teisę į privatumą. Visais atvejais labai svarbu, kad priemonės būtų proporcingos ir asmenų teisės nebūtų nepagrįstai ribojamos. Turi būti surastas balansas.

– **Kibernetinio saugumo, kaip integralios nacionalinio saugumo dalies, principas**.

Šis principas būtinas užtikrinti kibernetinio saugumo svarbą ir vietą tarp kitų valstybės prioritetų.

Šiuo metu Lietuvoje kibernetinis saugumas, kibernetinio saugumo užtikrinimas turi fragmentiškumo, kibernetinis saugumas kaip vienas iš prioritetų neminimas Nacionalinio saugumo pagrindų įstatyme. Kibernetinis saugumas nėra integruotas į nepaprastųjų situacijų valdymą Lietuvoje, netgi galima teigti, kad nepaprastųjų situacijų valdyme, atitinkamame teisiniame reguliavime, kuris nustato nepaprastųjų situacijų valdymo elementus valstybėje, kibernetinis saugumas kol kas neegzistuoja iš viso. Taigi, kibernetinis saugumas šiuo metu Lietuvoje egzistuoja daugiau kaip atskiras institutas. Nors kibernetinio saugumo integravimo elementų į nacionalinį saugumą Lietuvoje jau randasi (kaip pavyzdys – egzistuojanti Lietuvos nacionalinio saugumo strategija, kurioje kibernetinis saugumas įvardijamas kaip vienas iš Lietuvos prioritetų), visgi tai nepakankama. Pavyzdžiui, yra parengtas Nacionalinio saugumo strategijos projektas[33], jame numatoma reglamentuoti kibernetinio saugumo stiprinimą, apibrėžiamos kibernetinės grėsmės, tačiau vis tiek trūksta kibernetinio saugumo kategorijos integravimo į kitas su nacionaliniu saugumu susijusias sritis, pvz., socialinę apsaugą.

– **Bendradarbiavimo, įskaitant viešojo ir privačiojo sektorių (bei trečiojo sektoriaus), principas**.

Šis principas svarbus atsižvelgiant į kibernetinio tinklo specifiką, t.y. šiam tinklui nėra svarbios geografinės teritorijos, nacionalinių valstybių sienos ar žinybinis priklausymas, todėl norint pasiekti teigiamų rezultatų būtina stiprinti visas grandis, nes sistemos saugumas yra vertas tiek, kiek verta sistemos silpniausia grandis. Išorinio ir vidinio bendradarbiavimo kontekste visos bendradarbiaujančios grandys yra tarpusavyje priklausomos, todėl privalo derinti savo interesus.

33 Nutarimo dėl LR Seimo 2002 m. gegužės 28 d. nutarimo Nr. IX-907 „Dėl nacionalinio saugumo strategijos patvirtinimo“ pakeitimo projektas, LR Seimas, 2016. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/407015b094f311e68adcda1bb2f432d1?jfwid=-wd7z8nw39

Galima teigti, kad tai yra vienas iš pagrindinių principų užtikrinant kibernetinį saugumą. Kibernetinio saugumo reiškinys tapo globaliu, kibernetinės grėsmės neturi geografinių sienų, vyksta atakos iš trečiųjų valstybių. Todėl be bendradarbiavimo tarptautiniu ar regioniniu mastu, arba su užsienio valstybėmis (tiek prevencijos, tiek incidentų užkardymo / suvaldymo, tiek tyrimo kontekste) kibernetinio saugumo užtikrinimas sunkiai įmanomas. Lietuvai toks bendradarbiavimas yra ypač aktualus, kadangi Lietuva pasižymi labiausiai pralaidžiais elektroninių ryšių tinklais, dėl ko Lietuva tampa puikiu taikiniu. Lietuvai išskirtinai aktualus bendradarbiavimas su NATO, tačiau taip pat paminėtinas bendradarbiavimas su ES valstybėmis, ESBO, JT, taip pat bendradarbiavimas per neformalias grupes, konferencijas ir pan. Vykdant tarptautinį bendradarbiavimą, svarbu taip pat patiems veikti tarptautinę aplinką, būti proaktyviems, netgi formuoti tarptautinę aplinką kibernetinio saugumo srityje.

Taip pat kibernetinio saugumo užtikrinimas yra sunkiai įgyvendinamas be bendradarbiavimo valstybės viduje. Toks bendradarbiavimas gal būti įvairių atmainų: tarp institucijų, tarp viešojo ir privataus sektoriaus, su mokslo institucijomis ir kt. Taip pat akcentuotinas taip vadinamo „civilinio“ sektoriaus ir karinio sektoriaus bendradarbiavimas (angl. *civil and military cooperation*). Ypač svarbus viešojo ir privataus sektoriaus bendradarbiavimas, kuris tarptautinių ekspertų įvardijamas kaip pagrindas kibernetiniam saugumui užtikrinti. Lietuvoje toks bendradarbiavimas aktualizuojasi vien dėl to fakto, kad didžioji dauugma elektroninių ryšių infrastruktūros priklauso privačiam sektoriui.

Bendradarbiaujant kibernetinio saugumo srityje, papildomai turi būti siekiama laikytis lygiateisiškumo principo, t.y. vienos iš bendradarbiaujančių pusių interesai ir jų įgyvendinimas neturi esminiai viršyti kitos pusės interesų ir jų įgyvendinimo. Kitaip tariant, turėtų būti siekiama užtikrinti teisių ir pareigų balansą.

– **Asmeninės atsakomybės principas**.

Šis principas nurodo, kad didelė dalis kibernetinio saugumo priklauso nuo individų veiksmų naudojantis kibernetine erdve ir jos priemonėmis.

Principas svarbus tame kontekste, kad kiekvienas kibernetinio saugumo dalyvis turi būti atsakingas už kibernetinio saugumo palaikymą, įskaitant ir institucijų atsakomybę.

Šis principas Lietuvai ypač aktualus, kadangi individo asmeninė atsakomybė užtikrinant kibernetinį saugumą mažai aptariama. Individo asmeninės atsakomybės svarba pastaruoju metu vis auga. Plinta daiktų internetas, atsiranda vis daugiau įrenginių, prijungtų prie interneto, kuriuos valdo atskiri individai. Tuo tarpu įrenginiai, jei juose nustatyta silpna apsauga ar, pavyzdžiui, nėra pakeičiami gamykliniai slaptažodžiai[34], gali būti užkrečiami kenkėjiškomis programomis ir lengvai panaudoti pavyzdžiui DDoS atsakoms vykdyti, netgi atakoms prieš pačią valstybę.

Šis principas yra susijęs su asmeninio dalyvavimo principu. Visi individai turi ne tik jaustis atsakingi už kibernetinį saugumą, tačiau ir patys imtis aktyvių veiksmų užtikrinant kibernetinį saugumą. Turi būti jaučiama atsakomybė plačiąja prasme – ne tik už patį save, bet ir už kitus. Ir tokį atsakomybės supratimą reikia propaguoti kaip galima didesniam individų kiekiui.

Tamprios principo sąsajos su visuotinės gynybos įpareigojimu.

34 Kuriuos galima itin lengvai atspėti.

– **Proporcingumo principas**.

Šio principo dėka privalo būti vertinamos priemonės, resursai ir kylanti ar potenciali rizika.

Lietuva, kaip pakankamai maža valstybė, neturi vien kopijuoti didžiųjų valstybių patirtį kibernetinio saugumo prasme. Didžiosios valstybės, tokios, kaip JAV, JK, Vokietija ir kt., turi nepalyginamai daugiau resursų, tuo tarpu Lietuvos resursai yra daug labiau riboti. Tai reiškia, kad Lietuva turimus resursus kibernetiniam saugumui užtikrinti turi panaudoti kaip galima efektyviau, vertinant konkrečias nacionalines Lietuvos galimybes.

– **Inovacijų, tyrimų ir vystymo (research and development) skatinimo principas**.

Šis principas būtinas atsižvelgiant į technologinę kibernetinio saugumo prigimtį. Kibernetinio saugumo užtikrinimui turi būti įgyvendinamos pažangiausios technologijos ir reaguojama į naujausias grėsmes.

Lietuvos kaip valstybės stiprybė ir vienas iš pranašumų gali būti aktyviai diegiamos inovacijos. Tuo reikia pasinaudoti. Egzistuojantis vienas iš dabartinių ES kibernetinio saugumo tikslų, susijusių su inovacijų pritraukimu į pačią ES, ES produktų ir paslaugų kibernetinio saugumo kontekste, vystymu, gali labai derėti su Lietuvos potencialu ir galimybėmis.

Šis principas gali užtikrinti didesnį efektyvumą kovojant su kibernetinėmis grėsmėmis. Turint omenyje, kad Lietuva labai patraukli kibernetiniams nusikaltėliams, Lietuvai reikia ieškoti kaip galima efektyvesnių būtų kibernetiniam saugumui užtikrinti. Grėsmės modernėja, o tai reiškia, kad modernėjančioms grėsmės reikia ir atitinkamo atsako. Lietuva šiame kontekste negali sustoti. Reikia užtikrinti pastovų procesą, vystant tyrimus kibernetinio saugumo srityje ir diegiant inovacijas. Šio principo įgyvendinimas gali užtikrinti ir labai reikalingą kibernetinio saugumo srityje proaktyvų požiūrį.

– **Visapusiškumo, integralumo, proaktyvumo, solidarumo principai** yra svarbūs siekiant įvertinti kibernetinio saugumo kompleksiškumą ir taikyti efektyviausias priemones.

Šie principai yra kompleksinio pobūdžio ir pasižymi likusiais baziniais elementais, kurie reikalingi kiekvienai moderniai nacionalinei kibernetinio saugumo strategijai. Ne išimtis – ir Lietuva.

4. KIBERNETINIO SAUGUMO TIKSLAI, PAGRINDINĖS VEIKSMŲ SRITYS IR PRIORITETAI

Kibernetinio saugumo strategijos tikslai:

- Penkeriems metams užtikrinti tinkamą ir savalaikę galimų elektroninės erdvės grėsmių prevenciją Lietuvoje.
- Laipsniškai didinti atsakingų kontroliuojančių pajėgų skaičių, kryptingai didinant vartotojų informatyvumą ir pasitikėjimą elektronine erdve.
- Numatyti centralizuotą, skirtingus valstybinius segmentus ir lygius apimantį, proaktyvų kibernetinės gynybos planą.

Pagrindinės veiksmų sritys

Ypatingos svarbos informacinės infrastruktūros apsauga	Valstybės informacinių išteklių apsauga	Privataus ir viešo sektoriaus bendradarbiavimas	Institucinės sistemos išgrynimas	Kibernetinės kultūros vystymas	Tarptautinis bendradarbiavimas	Teisinės aplinkos vystymas
Prioritetai:						
Užtikrinti svarbiausių paslaugų visuomenei teikimą (kiekšių paslaugų teikimas susijęs su informacinėmis sistemomis), taip pat informacinių paslaugų teikimą. Parengties, reagavimo ir atkūrimo priemonės. Skirti atskirą dėmesį pramoninių procesų valdymo sistemoms. Ypatingos svarbos informacinės infrastruktūros turėtojų centralizuota sprendimų priėmimo ir valdymo sistema. Ypatingos svarbos informacinės infrastruktūros apsaugos metodų apibrėžimas. Gerosios kitų valstybių praktikos surinkimas, perkėlimas ir panaudojimas Lietuvos Respublikoje.	Užtikrinti valstybės informacinių išteklių apsaugą. Užtikrinti pažangių saugumo sprendimų įgyvendinimą. Organizacinių ir techninių apsaugos priemonių diegimas. Finansavimo minėtoms priemonėms paieška. Vykdomas gerosios praktikos formavimas. Kibernetinio saugumo specialistų pritraukimas.	Užtikrinti tinkamą naujai ruošiamų specialistų kompetenciją ir formuoti reikiamus įgūdžius. Užtikrinti bendradarbiavimą su privačiu sektoriumi. Užtikrinti kibernetinių grėsmių valdymą viešajame ir privačiame sektoriuose. Užtikrinti bendrą nacionalinės stebėjimo ir monitoringo sistemos veikimą. Vystomos galimybės plėtoti jau esamą privataus ir viešo sektorių bendradarbiavimo struktūrą. Vystomos galimybės novatoriškam smulkiajam kibernetinio saugumo srities verslui paprasčiau gauti finansavimą.	Užtikrinti pranešimų apie teisės pažeidimus elektroninėje erdvėje veikimą. Nustatoma viena pagrindinė institucija, atsakinga už kibernetinį saugumą Lietuvoje. Esamoms institucijoms priskirtų funkcijų peržiūra bei pakoregavimas pagal aktualijas.	Užtikrinti kibernetinio saugumo politikos formavimą, atsižvelgiant į tarptautinę patirtį. Užtikrinti informacinių paslaugų vartotojų švietimą. Kibernetinio saugumo suvokimo didinimas bei praktiniai užsiėmimai. Visuomenės įtraukimo mechanizmai, savanorystės skatinimas. Kursų apie kibernetinį saugumą mokykloms bei universitetams parengimas ir programų įvedimas.	Užtikrinti tarptautinį bendradarbiavimą siekiant ypatingai svarbos informacinės infrastruktūros apsaugos. Užtikrinti tarptautinį bendradarbiavimą kovai su teisės pažeidimais elektroninėje erdvėje. Užtikrinti bendradarbiavimą su savo sąjungininkais ir partneriais.	Užtikrinti teisinės sistemos veikimą kibernetinio saugo srityje. Apjungti elektroninės informacijos saugos bei kibernetinio saugumo institutus bei atitinkamai parengti teisės aktų būtinus pakeitimus. Suvienodinti sąvokas visame teisiniame reguliavime. Ištirti Kibernetinio saugumo įstatymui įgyvendinti reikalingų teisės aktų suderinamumą ir aktualumą. Atlikti atitinkamai būtinus reglamentavimo pakeitimus.

Prioritetai:						
Finansavimo paieška techniniams ypatingos svarbos informacinės infrastruktūros sprendimams. Mokymai atsakingiems už tokią infrastruktūrą darbuotojams. Grėsmių valdymas, rizikos vertinimo planai.		Sustiprinamas ir racionalizuojamas bendradarbiavimas kibernetinio saugumo klausimais įvairiuose ekonomikos sektoriuose, įskaitant mokymą ir švietimą kibernetinio saugumo srityje. Mokslinio tyrimo ir plėtros planų vystymas. E-verslo skatinimas.				

4.1. Kibernetinio saugumo strategijos tikslai:

- Penkeriems metams užtikrinti tinkamą ir efektyvią kibernetinę gynybą, bei savalaikę galimų elektroninės erdvės grėsmių prevenciją Lietuvoje.
- Laipsniškai didinti atsakingų kontroliuojančių pajėgų skaičių, kryptingai didinant vartotojų informatyvumą ir pasitikėjimą elektronine erdve.
- Numatyti centralizuotą, skirtingus valstybinius segmentus ir lygius apimantį proaktyvų kibernetinės gynybos planą.

Tyrime dalyvavusių ir apklaustų ekspertų įžvalgos apie strategijoje turintį būti strateginį tikslą (ar kelis) yra skirtingos. Vieni ekspertai išskiria tik vieną tikslą, tiesiogiai nukreiptą į kritinės informacinės infrastruktūros nepertraukiamą funkcionavimą ir kuo greitesnį galimų pasekmių likvidavimą. Yra ekspertų, pasisakančių už daugiau tikslų, net išskiria galimas tikslų dedamąsias: užtikrinti saugumą; užtikrinti laisvos raiškos galimybę; užtikrinti socialinius-ekonominius privalumus; nustatyti saugotinų objektų sąrašą; nustatyti, nuo ko objektus reikia saugoti; nustatyti, kaip saugoti tuos objektus. Formuojant tikslus taip pat galima užduoti atitinkamus klausimus: kokios atakos turi būti atlaikomos, kiek laiko turi atlaikyti ir per kiek laiko turi būti reaguojama į kiekvieną incidentą. Yra dar viena aktuali sritis – edukacija ir švietimas, ekspertai išskyrė ir šią sritį.

Bendrai paminėtina, kad tiek formuluojant tikslus, tiek pagrindines veiksmų sritis ar prioritetus, turi būti laikomasi holistinio (t.y. visaapimančio) požiūrio. Šiuo metu tokio požiūrio trūksta, išskiriamos atskiros sritys, ir nors jos yra labai svarbios, kibernetinis saugumas ir kibernetinė gynyba turi būti vystomi kompleksiškai, įtraukiant visas suinteresuotas šalis, užtikrinant švietimą, mokslinius tyrimus, skatinant investicijas, šviečiant visuomenę ir pan.

4.2. Pagrindinės veiksmų sritys

Lietuvos kibernetinio saugumo strategijoje turėtų būti išskiriamos šios **pagrindinės veiksmų kryptys**:

1. Kritinės infrastruktūros apsauga;
2. Valstybės informacinių išteklių apsauga;
3. Privataus ir viešo sektoriaus bendradarbiavimas;
4. Institucinės sistemos išgryninimas;
5. Kibernetinės kultūros vystymas;
6. Tarptautinis bendradarbiavimas;
7. Teisinės aplinkos vystymas.

1. Kritinės infrastruktūros apsauga

Lietuvos Respublikoje nuo 2008 m. buvo išreikštas susirūpinimas dėl kritinės infrastruktūros apsaugos. Atsižvelgdama į gerąją kitų valstybių praktiką ir poreikį turėti nacionalines strateginio lygmens gaires kibernetinio saugumo srityje, tarpžinybinė darbo grupė dar 2008 metų lapkričio mėnesį pasiūlė Vyriausybei inicijuoti šių strategijų rengimą: Lietuvos kibernetinio saugumo ir Lietuvai ypatingai svarbios infrastruktūros apsaugos[35]. Mokslinio projekto tyrime dalyvavę kibernetinio saugumo ekspertai iš Lietuvos taip pat išskyrė kritinės infrastruktūros apsaugą kaip vieną iš pagrindinių Lietuvos Respublikos kibernetinio saugumo veiksmų krypčių. Jie taip pat paminėjo kritinės infrastruktūros sąrašo parengimą kaip vieną pagrindinių šios krypties prioritetinių veiksmų. Kitas svarbus žingsnis po sąrašo parengimo – apsaugos metodų išgryninimas bei įtvirtinimas. LR Valstybės kontrolės išankstinėje ataskaitoje paminėta, kad valstybės ir savivaldybių elektroninių ryšių tinklų ir informacinių sistemų saugumą reglamentuoja ne įstatymai, o Vyriausybės nutarimai, ministrų įsakymai, kuriuose nurodoma, kad Vyriausybei nepavaldžioms institucijoms ir įstaigoms jie yra tik rekomendacinio pobūdžio[36]. Nėra aiškumo, kaip turėtų būti apsaugota kritinė infrastruktūra Lietuvos Respublikoje, kokie konkretūs stebėsenos bei reagavimo mechanizmai turėtų būti įtvirtinti. Todėl svarbu kibernetinio saugumo strategijoje apibrėžti kritinės infrastruktūros apsaugos metodus, gerosios kitų valstybių praktikos panaudojimą Lietuvos Respublikoje, finansavimo paieška techniniams kritinės infrastruktūros sprendimams. Šalia teorinės reikalavimų dalies nustatymo turėtų būti organizuojami mokymai, procesų perėmimai pagal geriausias praktikas.

2. Valstybės informacinių išteklių apsauga

Valstybiniame sektoriuje visų pirma akcentuojama valstybės informacinių išteklių apsauga, informacinės saugos spragos, taip pat, kokių priemonių reikia imtis, kad būtų užtikrinta visapusiška valstybės informacinių išteklių apsauga. LR Valstybės kontrolės išankstinėje ataskaitoje taip pat pažymėta, kad Lietuvoje nėra sukurta strateginės elektroninės informacijos saugos stebėsenos sistema ir nepakankamai apibrėžta šią sritų koordinuojančių institucijų kompetencija[37]. 2015 m. LR Valstybės kontrolės audito ataskaitoje nurodoma, kad išanalizavus 18-kos įstaigų patikrų vietoje rezultatus buvo nustatyta, kad kibernetinio saugumo organizacinių ir techninių priemonių įgyvendinimas viešajame sektoriuje yra nepakankamas, nes

35 Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės siūlymu šioje strategijoje turės būti apibrėžti ir ypatingos svarbos informacinės infrastruktūros nacionaliniu mastu apsaugos principai.

36 Išankstinio tyrimo ataskaita. Strateginės informacijos sauga. LR valstybės kontrolė. 2009. Žiūrėta 2016 10 29// www.vkontrole.lt.

37 Ten pat.

šiose įstaigose vidutiniškai taikoma 25 proc. kibernetinei saugai užtikrinti rekomenduojamų organizacinių priemonių (13 proc. jų taikoma iš dalies) ir tinkamai įgyvendinama tik 39 proc. kibernetiniai saugai užtikrinti rekomenduojamų techninių priemonių (22 proc. jų įgyvendinama iš dalies)[38]. Manytina, jog valstybinio sektoriaus apsauga – turėtų būti viena iš Lietuvos kibernetinio saugumo strategijoje apibrėžiamų pagrindinių krypčių. Šį teiginį taip pat paminėjo ir Lietuvos ekspertai, nurodydami valstybės išteklius kaip vieną iš svarbiausių saugotinų objektų nuo kibernetinių atakų. Šioje srityje turėtų būti toliau diegiamos organizacinės ir techninės apsaugos priemonės, organizuojama finansavimo minėtų priemonių paieška, vykdomas gerosios praktikos formavimas, specialistų pritraukimas, specialistų mokymai.

3. Privataus ir viešo sektoriaus bendradarbiavimas

2016-07-05 Europos Komisija ir Europos kibernetinio saugumo organizacija (ECSO) pasirašė viešojo ir privačiojo sektorių kibernetinio saugumo partnerystės susitarimą. Šiuo dokumentu skatinamas bendradarbiavimas tarp viešojo ir privačiojo sektorių atstovų ankstyvosiose mokslinių tyrimų ir inovacijų proceso stadijose. Be to, suderinama kibernetinio saugumo rinkos paklausa ir pasiūla pagal galutinių vartotojų ir svarbių sektorių (pvz. energetika, sveikata, transportas, finansai) reikalavimus. Lietuvos Respublikos kibernetinio saugumo strategijoje ši kryptis taip pat turėtų būti numatyta kaip viena iš krypčių. Tos pačios nuomonės laikėsi ir Lietuvos kibernetinio saugumo ekspertai.

Šioje srityje turėtų būti vystomos galimybės plėtoti jau esamą privataus ir viešo sektorių bendradarbiavimo struktūrą, taip pat vystomos galimybės novatoriškam smulkiajam kibernetinio saugumo srities verslui paprasčiau gauti finansavimą; sustiprinamas ir racionalizuojamas bendradarbiavimas kibernetinio saugumo klausimais įvairiuose ekonomikos sektoriuose, įskaitant mokymą ir švietimą kibernetinio saugumo srityje.

Privataus ir viešojo sektoriaus bendradarbiavimo mastą reikėtų derinti su valstybės ir / ar atitinkamų institucijų / įskaitų bei privataus sektoriaus finansinėmis galimybėmis.

4. Institucinės sistemos išgrynimas

Lietuvos Respublikoje pastebima institucijų, atsakingų už kibernetinį saugumą fragmentacija. 2011 m. LR Vyriausybės nutarime dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos patvirtinimo įvardijama daugybė institucijų, atsakingų už kibernetinį saugumą Lietuvoje. LR Kibernetinio saugumo įstatyme apibrėžtos kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos, jų įgaliojimai, tačiau trūksta kompetencijos atskyrimo formuojant ir įgyvendinant kibernetinio saugumo ir el. informacijos saugos politiką, neperžiūrėtos vykdomos funkcijos, kurios nebeatitinka pasikeitusio reglamentavimo[39]. Deja, bet kai atsakingų institucijų yra daug, sunku tikėtis gero rezultato. Tokią pačią poziciją yra išreiškusi ir Lietuvos Respublikos Prezidentė Dalia Grybauskaitė[40]. Jos nuomone, turėtų būti nustatoma viena pagrindinė institucija, atsakinga už kibernetinį saugumą Lietuvoje. Kuo daugiau įstaigų yra atsakingos už el. informacijos saugos sričių valdymą, koordinavimą ir priemonių nustatymą, tuo sudėtingiau šioje srityje formuoti nuoseklią valstybės valdymo politiką, suderinti skirtingų institucijų valdymo interesus, užtikrinti tinkamą lėšų panaudojimą.

38 Valstybinio audito ataskaita. Kibernetinio saugumo aplinka Lietuvoje. LR valstybės kontrolė. 2015. Žiūrėta 2016 10 29// www.vkontrole.lt

39 Ten pat.

40 Prezidentė Dalia Grybauskaitė: informacinė apsauga turi būti vykdoma operatyviai ir koordinuotai. Interneto dienraštis 15min.lt. 2016. Žiūrėta 2017 02 15. http://www.15min.lt/naujiena/aktualu/lietuva/dalia-grybauskaite-informacine-apsauga-turi-buti-vykdoma-operatyviai-ir-koordinuotai-56-341758

Taip pat, viena iš problemų Lietuvoje, susijusi su institucine sistema – Nacionalinis kibernetinio saugumo centras yra Lietuvos Respublikos Krašto apsaugos ministerijos struktūrinis padalinys ir stokoja savarankiškumo funkcinės priklausomybės prasme.

Autorių nuomone, institucinės sistemos išgryninimas turėtų būti kaip vienas iš Lietuvos kibernetinio saugumo strategijoje apibrėžiamų pagrindinių krypčių.

5. Kibernetinės kultūros vystymas

Lietuvos Respublikoje „kibernetinė kultūra“ dar tik pradedama vystyti. Atrodytų, kad visų pirma reikėtų susitvarkyti su esminiais dalykais, kaip kritinės infrastruktūros identifikavimu, apsaugos būdais; valstybinių institucijų apsauga, institucijų funkcijų išgryninimu. Tačiau, kita vertus, lygiagrečiai svarbus dėmesys turėtų būti skiriamas kibernetinės kultūros vystymui.

LR Nacionalinio saugumo pagrindų įstatyme nustatytas visuotinės gynybos principas taikytinas ir elektroninėje erdvėje bei įpareigoja netgi kiekvieną pilietį (elektroninėje erdvėje – kiekvieną elektronine erdve besinaudojantį pilietį) užtikrinti aktyvią gynybą. Gynyba elektroninėje erdvėje turėtų prasidėti nuo kiekvieno piliečio indėlio į bendrąją kibernetinio saugumo situaciją. Pavyzdžiui, kuo mažiau bus užkrėstų kompiuterių, tuo mažesnė tikimybė, kad šie kompiuteriai bus panaudoti DDoS atakoms prieš Lietuvos institucijas. Taigi, tam kad užtikrinti kibernetinį saugumą asmeniniame lygyje, reikia turėti atitinkamas žinias, pvz., kaip pasikeisti slaptažodžius, kaip užtikrinti įrenginių minimalią apsaugą nuo virusų ir kt. Tam reikia vykdyti švietimo veiksmus.

Švietimas apie kibernetinį saugumą turėtų būti įtrauktas į mokyklos, universiteto programas. Tokia nuomonė buvo patvirtinta ir Lietuvos Respublikos ekspertų, dirbančių su kibernetiniu saugumu. Jų teigimu, švietimas, akcentuojant vartotojų žinojimą bei supratimą apie kibernetinio saugumo problematiką, turėtų būti viena pagrindinių Lietuvos kibernetinio saugumo strategijoje apibrėžiamų pagrindinių krypčių. Kitų valstybių strategijose kibernetinio saugumo suvokimo didinimas bei praktiniai užsiėmimai – įprasta (Austrijos, Belgijos, Čekijos, Danijos, Olandijos ir kitų valstybių) strategijų dalis.

Švietimo, informuotumo didinimo ir mokymo programos turi būti pastoviai vystomos ir atnaujinamos, atsižvelgiant į besikeičiančią kibernetinio saugumo situaciją ir besikeičiančias kibernetines grėsmes. Turėtų būti kuriamos bei palaikomos ir naujos studijų programos. Tiek Lietuvoje, tiek aplinkinėse valstybėse šiuo metu rengiama daug techninio profilio specialistų, tačiau trūksta specialistų, turinčių vadybines, teisines žinias, sugebančių valdyti kibernetinio saugumo procesus.

Taip pat, turi būti vystoma mokymosi visą gyvenimą koncepcija. O švietimą, pagal realias galimybes, turi vykdyti kuo platesnis subjektų ratas.

Kibernetinės kultūros kontekste labai svarbūs visuomenės įtraukimo mechanizmai. Turi būti skatinama savanorystė užtikrinant kibernetinį saugumą. Tačiau ši savanorystė turi būti kontroliuojama, tikslu išvengti savanorystės veiksmų peraugimo į neteisėtas veikas.

6. Tarptautinis bendradarbiavimas

Nuoseklios tarptautinės ES elektroninės erdvės politikos nustatymas – ES kibernetinio saugumo strategijos prioritetinė sritis[41]. Atsižvelgiant į grėsmes nacionaliniam saugumui, įvardintas LR Valstybės saugumo

41 ES kibernetinio saugumo strategija. 2013. Prieiga per internetą: http://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52013JC0001&from=LT

departamento[42], kibernetinis šnipinėjimas prieš Lietuvos valstybės institucijas, šalies kritinės infrastruktūros objektus, privatųjį sektorių išlieka viena pagrindinių grėsmių šalies nacionaliniam saugumui. Panašios grėsmės gali būti identifikuojamos ir mūsų valstybių kaimynių, todėl mes galime kalbėti apie Baltijos šalių bendradarbiavimą kibernetinio saugumo srityje kovojant bei atsižvelgiant į dabartinę geopolitinę situaciją. Be to, kibernetiniai nusikaltimai yra be sienų, todėl tarptautinis bendradarbiavimas ir globaliu lygmeniu, autorių nuomone – turėtų būti viena iš pagrindinių Lietuvos kibernetinio saugumo strategijoje apibrėžiamų pagrindinių krypčių. Ta pati nuomonė buvo patvirtinta ir Lietuvos kibernetinio saugumo ekspertų.

7. Teisinės aplinkos vystymas

Lietuvos Respublikoje numatyta teisinė bazė kibernetinio saugumo sričiai yra gana fragmentiška. Kaip nustatyta 2015 m. LR Valstybės kontrolės audito ataskaitoje, kibernetinio saugumo ir el. informacijos saugos reguliavimas turi trūkumų[43]. Autorių nuomone, viena didžiausių problemų yra tai, jog skirtinguose teisės aktuose (2011 m. LR Vyriausybės nutarime dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos patvirtinimo ir 2015 m. LR Kibernetinio saugumo įstatymuose) yra įtvirtinti atskiri institutai – elektroninės informacijos saugos bei kibernetinio saugumo.

Elektroninės informacijos saugos institutas didžiąja dalimi paremtas elektroninės informacijos konfidencialumu. Tuo tarpu, kibernetinio saugumo institutas daugiau paremtas integralumo bei prieinamumo užtikrinimu. Turint omenyje taip vadinamą klasikinę CIA triadą, elektroninės informacijos sauga laikytina kibernetinio saugumo dalimi, kai kibernetinis saugumas papildomai apima jurisdikcijos ir kitus klausimus[44].

Vystant kibernetinio saugumo srities teisinį reglamentavimą, visų pirma reikėtų svarstyti šių institutų apjungimą, suvienodinant sąvokas, nustatant vieningą apjungtos saugumo srities valdymą. Tačiau įgyvendinimo lygmenyje (t.y. informacinių sistemų kūrimas ir kt.) ir toliau galėtų likti tam tikri skirtumai, kuriuos dalinai lemia ir atitinkamų saugos srities standartų egzistavimas bei taikymas.

Taip pat, reikėtų ištirti Kibernetinio saugumo įstatymui įgyvendinti reikalingų teisės aktų (plačiąja prasme, įskaitant ir elektroninės informacijos saugos institutą) suderinamumą ir aktualumą.

4.3. Prioritetų turinys

Papildomai prie pagrindinių svarbių veiklos sričių „karštųjų prioritetų“ galime detalizuoti kitus, dalinai iš ekspertų apklausos išplaukiančius prioritetus, kurių detalesnis turinio atskleidimas leis tinkamai juos įkomponuoti į numatomą kibernetinio saugumo strategijos modelį.

1. **Svarbios kritinės infrastruktūros apsauga, paslaugų vartotojams užtikrinimas.**
   Elektroninių viešųjų ir komercinių paslaugų skaičius Lietuvoje nuolatos auga. Nuo esamų ir naujai atsirandančių paslaugų tiesiogiai priklauso ekonominė valstybės ir gyventojų gerovė, administracinių paslaugų teikimas, teisinės ir politinės sistemos funkcionavimas. Vartotojai įprato dalį paslaugų gauti elektroniniu būdu, tokių paslaugų trikdis, neveikimas gali atnešti didelius nuostolius privačiam

42 Grėsmių nacionaliniam saugumui vertinimas. Lietuvos Respublikos Valstybės saugumo departamentas ir antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, Vilnius, 2016. Žiūrėta 2016 09 26// http://www.vsd.lt/Files/Documents/635948635773762500.pdf.

43 Valstybinio audito ataskaita. Kibernetinio saugumo aplinka Lietuvoje. LR valstybės kontrolė. 2015. Žiūrėta 2016 10 29// www.vkontrole.lt

44 ITU NATIONAL cybersecurity guide. International telecommunication union. 2011. P. 13. Žiūrėta 2016 10 29//http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

ir viešam sektoriui, paveikti valstybės reputaciją. Strategija turi numatyti konkrečius veiklos metodus, kurie leis užtikrinti nepertraukiamą svarbių informacinių paslaugų teikimą.

a. Užtikrinti svarbiausių paslaugų visuomenei teikimą (kiek šių paslaugų teikimas susijęs su informacinėmis sistemomis), taip pat informacinių paslaugų teikimą

   Vis didesnis vartotojų skaičius naudojasi elektroninėmis paslaugomis, kurios būtinos jų darbo funkcijų atlikimui. Valstybės prioritetas – elektroninės viešosios paslaugos.

   Turi būti nustatytos parengties, reagavimo ir atkūrimo priemonės. Skirti atskirą dėmesį pramoninių procesų valdymo sistemoms.

b. Kritinės infrastruktūros turėtojų centralizuota sprendimų priėmimo ir valdymo sistema

   Atsakinga institucija, turinti galimybę koordinuoti ir centralizuotai nustatyti veiklos standartus, reikiamus vidinės organizacijos struktūrinius pokyčius, audituoti kibernetinės saugos procesus. Procesų vienodumas ir jų taikymas leidžia greitai pastebėti esminius trūkumus.

c. Kritinės infrastruktūros apsaugos metodų apibrėžimas

d. Užtikrinti valstybės informacinių išteklių apsaugą

   Technologinė infrastruktūra turi būti apsaugota nuo galimų grėsmių, itin svarbūs duomenys turi būti atskirti ir saugomi saugiuose duomenų centruose. Konsoliduojant valstybės registrus reikia suprasti, kad viename taške esantys svarbūs duomenys gali būti pažeidžiami. Naudojant konkrečius pasirinktus apsaugos būdus ir techninius sprendimus visuose registruose sudėtinga užtikrinti itin svarbių duomenų apsaugą, todėl reikia galvoti apie tokių duomenų fizinį atskyrimą ir rezervo perkėlimą į kitoje fizinėje vietoje esančias informacines sistemas (nebūtinai Lietuvos teritorijoje).

e. Užtikrinti kibernetinių grėsmių valdymą viešajame ir privačiame sektoriuose

   Kvalifikuotas personalas, paruoštos metodikos, specialiosios mokymo programos. Nuolatinis monitoringas naujų sričių, paslaugų, į kurias gali būti nukreipta ataka. Taip pat būtina savalaikė rizikos vertinimo sistema (bei planas), nuolatos atnaujinama, tikrinama. Taip pat tokios sistemos valdymo mechanizmas. Tai galėtų būti centralizuotai parengta ir tinkama įstaigoms (pagal konkretų profilį).

f. Užtikrinti bendrą nacionalinės stebėjimo ir monitoringo sistemos veikimą

   Institucijų, verslo vienetų, paprastų vartotojų teisėta veiklos priežiūra. Reagavimas realiu laiku į grėsmes, keliančias grėsmę valstybei ar atskiram vartotojui.

g. Užtikrinti tarptautinį bendradarbiavimą siekiant ypatingai svarbios informacinės infrastruktūros apsaugos

   Tarptautinis bendradarbiavimas padeda užtikrinti sklandų svarbių informacinių infrastruktūros mazgų darbą, kartu su esamais partneriais, ekspertais ir sąjungininkais galima garantuoti nepertraukimą paslaugų teikimą.

h. Gerosios kitų valstybių praktikos surinkimas, perkėlimas ir panaudojimas Lietuvos Respublikoje..

i. Finansavimo paieška techniniams kritinės infrastruktūros sprendimams.

j. Mokymai atsakingiems už kritinę infrastruktūrą darbuotojams.

k. Grėsmių valdymas, rizikos vertinimo planai.

2. Greita ir veiksminga reakcija į elektroninius teisės pažeidimus

Atsirandantys ekonominiai nuostoliai dėl elektroninių nusikaltimų mažina pasitikėjimą elektroninėmis paslaugomis. Tinkamos kvalifikacijos ir deramai paruošti specialistai gebės kvalifikuoti teisės

pažeidimus elektroninėje erdvėje. O vartotojų nuolatinis švietimas leis sumažinti šių teisės pažeidimų natūralų latentiškumą.

a. Užtikrinti pranešimų apie teisės pažeidimus elektroninėje erdvėje veikimą

   Siekiant pagerinti elektroninių teisės pažeidimų išaiškinimą, užkardymą, gyventojų tiesioginį prisidėjimą prie atskleidimo (savanorystė), būtina vystyti centralizuotą pranešimų sistemą.

b. Užtikrinti informacinių paslaugų vartotojų švietimą

   Be užkardymo ir kovos didelis dėmesys turi būti skiriamas vartotojams, kurie naudojasi informacinėmis paslaugomis. Būtina šviesti juos apie technines, teisines ir organizacines apsaugos priemones, rekomenduoti labiausiai apsaugotus techninius sprendimus, supažindinti su naujomis technologijomis.

c. Užtikrinti tarptautinį bendradarbiavimą kovai su teisės pažeidimais elektroninėje erdvėje

   Palaikyti ir tobulinti keitimosi informacija tarp šalių tvarkas ir procedūras, atnaujinti ryšius su valstybėmis, kurios nedalyvavo informacijos mainuose. Aktyviai dalyvauti tarptautiniuose projektuose ir iniciatyvose, kurios nukreiptos į tarptautinę kovą su elektroniniais teisės pažeidimas. Prisidėti prie paramos valstybėms sąjungininkėms, jei Lietuvos tarnybų turima kompetencija ir kvalifikacija gali prisidėti prie šalių partnerių geresnės elektroninės erdvės apsaugos.

d. Nustatoma viena pagrindinė institucija, atsakinga už kibernetinį saugumą Lietuvoje

e. Esamoms institucijoms priskirtų funkcijų peržiūra bei pakoregavimas pagal aktualijas

f. Mokslinio tyrimo ir plėtros planų vystymas.

g. E-verslo skatinimas.

3. Nuolatos kintančių kibernetinių grėsmių valdymas

Reikalinga užtikrinti savarankiškos institucijos veikimą, kuri remtųsi naujais kibernetinio saugumo veiklos metodais, taikytų savalaikius ir atnaujinamus techninius sprendimo būdus. Būtų aprūpinta tinkamą kvalifikaciją ir kompetenciją turinčiais darbuotojais.

a. Užtikrinti pažangių saugumo sprendimų įgyvendinimą

   Aktyviai bendradarbiauti su šios srities mokslinius tyrimus rengiančiais tyrėjais. Parenkant šiuos sprendimus taip pat bendradarbiauti su krašto apsaugos ir verslo rinkos dalyviais. Numatyti pastovų atnaujinimo darbų planą.

   Skatinti e-verslą, produktų kūrimą kibernetinio saugumo srityje.

b. Užtikrinti tinkamą naujai ruošiamų specialistų kompetenciją ir formuoti reikiamus įgūdžius

   Numatyti dirbantiems specialistams galimybę papildomai mokytis naujose programose. Teikti paramą naujai rengiamiems studentams. Organizuoti mokymus kartu su užsienio šalių ekspertais/lektoriais, turinčiais patirties rengiant kibernetinio saugumo specialistus.

   Svarbu skatinti savanorystę ir tokiu būdu papildomai kelti kvalifikaciją.

c. Užtikrinti bendradarbiavimą su privačiu sektoriumi

   Įmonės, kurios teikia informacines paslaugas, vysto technines apsaugos priemones, turi aktyviai dalyvauti kovoje su kibernetinėmis grėsmėmis. Būtina skatinti nacionalinių kompanijų naujų sprendimų kūrimą ir įdiegimą į nacionalinės gynybos sistemą, taip pat juos pristatyti tarptautiniams partneriams.

   Vystyti mokslinius tyrimus ir nustatyti plėtros planus.

d. Organizacinių ir techninių apsaugos priemonių diegimas

e. Kibernetinio saugumo suvokimo didinimas bei praktiniai užsiėmimai.
f. Kursų apie kibernetinį saugumą mokykloms bei universitetams parengimas ir programų įvedimas
g. Visuomenės įtraukimo mechanizmai, savanorystės skatinimas.
h. Vykdomas gerosios praktikos formavimas
i. Finansavimo minėtoms priemonėms paieška

4. Tarpinstitucinis ir tarptautinis valstybės įstaigų darbas

Siekiant pagerinti kovą su kibernetinėmis grėsmėmis Lietuvoje, tikslinga atnaujinti teisinę sistemą, skirtą reguliuoti atskirų institucijų kompetencijas kibernetinio saugumo srityje, numatyti aiškias veikimo ribas ir konkrečią atsakomybę, taip pat įgyvendinti bendradarbiavimą.

a. Užtikrinti teisinės sistemos veikimą kibernetinio saugumo srityje

   Įgyvendinant kibernetinio saugumo priemones, būtina peržiūrėti susijusius teisės aktus, esant būtinybei keisti tuos, kurie nėra aktualūs šiai dienai, neapima naujai atsirandančių sričių, arba nėra įmanoma pritaikyti funkcinio ekvivalentiškumo principo.

b. Apjungti elektroninės informacijos saugos bei kibernetinio saugumo institutus bei atitinkamai parengti teisės aktų būtinus pakeitimus
c. Užtikrinti kibernetinio saugumo politikos formavimą, atsižvelgiant į tarptautinę patirtį

   Vartotojai turi būti užtikrinti, kad siekiant užsibrėžtų tikslų, nebus pažeidžiamas asmens privatumas, konstitucinės asmens teisės. Strategijoje turi atsispindėti dalys stiprinančios pasitikėjimą taikomomis apsaugos priemonėmis elektroninėje erdvėje.

d. Užtikrinti tarpinstitucinį bendradarbiavimą

   Užtikrinti bendradarbiavimą tiek tarp atsakingų institucijų kibernetinio saugumo srityje, tiek tarp visų institucijų, kurioms numatytos teisės ar pareigos kibernetinio saugumo srityje. Šiuo metu tarpinstitucinis bendradarbiavimas yra viena iš silpnųjų vietų užtikrinant kibernetinį saugumą, ypač viešajame sektoriuje.

   Šiuolaikinių kibernetinių grėsmių kontekste bei turint omenyje geopolitinę situaciją, svarbu užtkrinti bendradarbiavimą tarp institucijų, kurios atsakingos už „išorinį saugumą“ ir institucijų, kurios atsakingos už „vidinį saugumą“.

e. Ištirti Kibernetinio saugumo įstatymui įgyvendinti reikalingų teisės aktų suderinamumą ir aktualumą.
f. Vystomos galimybės plėtoti jau esamą privataus ir viešo sektorių bendradarbiavimo struktūrą
g. Suvienodinti sąvokas visame teisiniame reguliavime.

   Būtina pagal galimybes suvienodinti ir taikyti vienodas sąvokas. Vienodos sąvokos leidžia atsakingiems subjektams tą patį reiškiinį traktuoti vienodai.

h. Užtikrinti bendradarbiavimą su savo sąjungininkais ir partneriais

   Būtina stiprinti bendradarbiavimą su kaimyninėmis šalimis, plėtoti bendradarbiavimo formas, plėsti ryšius su tokias formas turinčiomis šalimis. Dalyvauti ES bendros kibernetinio saugumo politikos plėtojime, taip didinant valstybių partnerių kibernetinio saugumo pajėgumus.

i. Vystomos galimybės novatoriškam smulkiajam kibernetinio saugumo srities verslui paprasčiau gauti finansavimą.
j. Sustiprinamas ir racionalizuojamas bendradarbiavimas kibernetinio saugumo klausimais įvairiuose ekonomikos sektoriuose, įskaitant mokymą ir švietimą kibernetinio saugumo srityje.

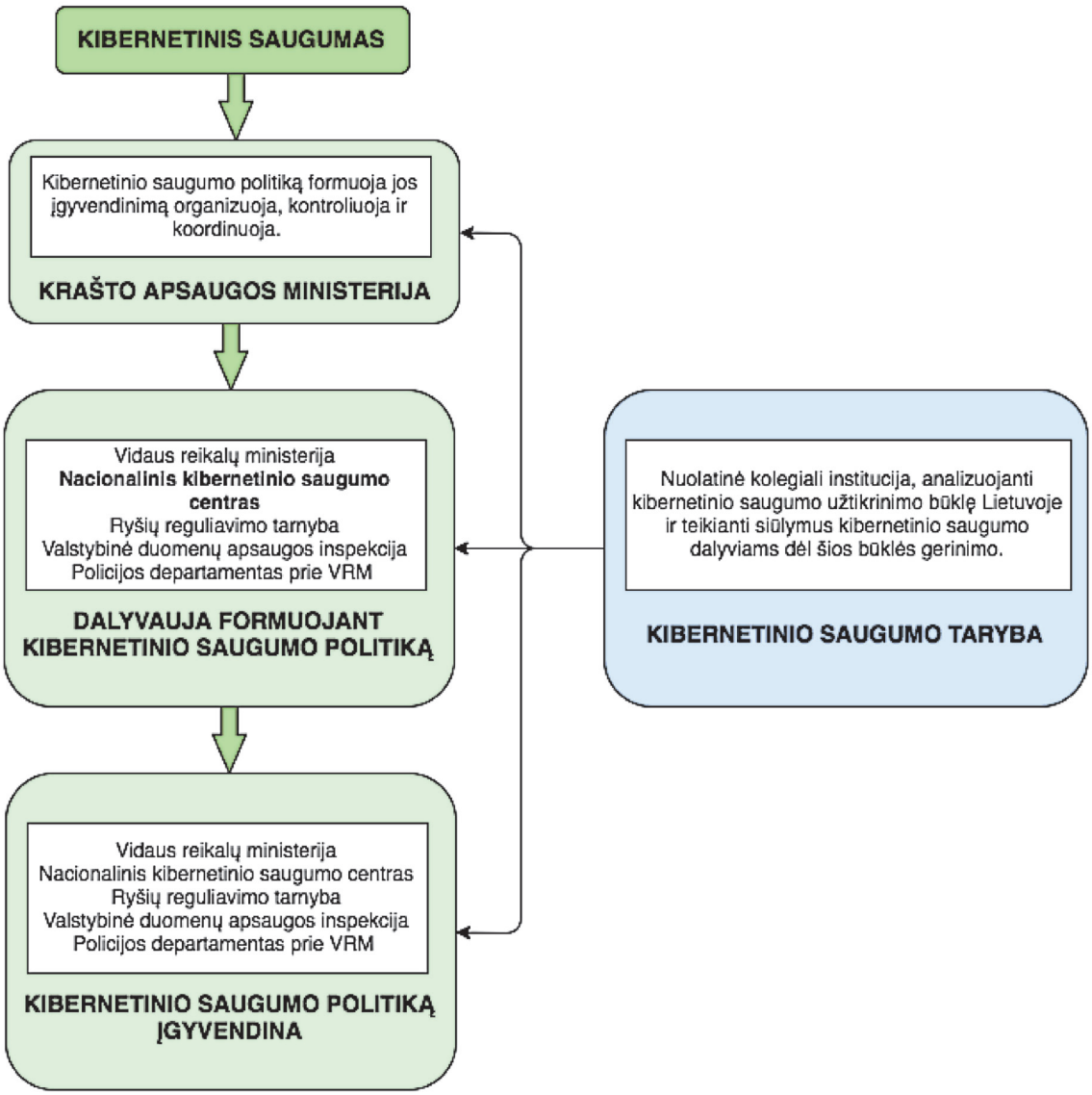
5. KIBERNETINIO SAUGUMO VALDYMO SISTEMA

Toliau aptariant kibernetinio saugumo valdymo sistemą, nėra detaliai nagrinėjamos visos įsitraukusios institucijos ir nėra detaliai aptariamos jų funkcijos. Žemiau pasisakoma tik dėl esminių kibernetinio saugumo valdymo sistemos elementų, t.y. atsakingos institucijos, politikos formavimo kibernetinio saugumo srityje ir patariamosios funkcijos.

Visų pirma, paminėtina Tinklų ir informacijos saugumo direktyva, kurios 7 straipsnyje nurodyta, kad nacionalinėje tinklų ir informacijos saugumo strategijoje be kitų klausimų, turi būti aptarta ir valdymo sistema, skirta nacionalinės tinklų ir informacinių sistemų saugumo strategijos tikslams ir prioritetams įgyvendinti, įskaitant valdžios įstaigų ir kitų atitinkamų subjektų vaidmenis ir įsipareigojimus.

Antra, dabartinę institucinę kibernetinio saugumo sistemą, nustatytą Lietuvos Respublikos kibernetinio saugumo įstatyme, galima pavaizduoti taip, kaip nurodyta žemiau.

Paveikslėlis Nr. 8. *Autorių sudaryta institucinė kibernetinio saugumo sistema Lietuvoje*



Šioje schemoje atvaizduotas struktūrinis Lietuvos Respublikos krašto apsaugos ministerijos padalinys – Nacionalinis kibernetinio saugumo centras – Lietuvos Respublikos kibernetinio saugumo įstatyme išskiriamas kaip atskira institucija. Tokia praktika yra ydinga dėl kelių priežasčių:

- Krašto apsaugos ministerija yra ne tik kibernetinio saugumo politiką formuojanti, jos įgyvendinimą organizuojanti, kontroliuojanti bei koordinuojanti institucija, bet taip pat ir viešojo administravimo subjektas, privalantis vykdyti įpareigojimus kibernetinio saugumo srityje, taip pat institucija. Tokios institucijos struktūrinis padalinys – Nacionalinis kibernetinio saugumo centras negali kontroliuoti, kaip institucija laikosi kibernetinio saugumo reikalavimų. T.y. ta pati institucija negali savęs kontroliuoti, o Krašto apsaugos ministrui negali nurodinėti vieno iš šios ministerijos struktūrinių padalinių vadovas. Turi būti nustatytas efektyvus kontrolės mechanizmas;
- Nacionaliniam kibernetinio saugumo centrui esant struktūriniam Krašto apsaugos ministerijos padaliniui, nėra atskirtos politikos formavimo ir kontrolės mechanizmai, funkcijos. Tokių funkcijų atskyrimas akcentuojamas pažangiausiose (kibernetinio saugumo užtikrinimo prasme) valstybėse, tokiose kaip Vokietija, Suomija ir kt.;
- Nacionalinio kibernetinio saugumo centro funkcijas vykdant vienam iš ministerijų struktūrinių padalinių, gali atsirasti veiklos koordinavimo su kitomis institucijomis ir nurodymų vykdymo problemos. Kaip rodo praktika, Lietuvoje šiuo metu ypač stinga tarpinstitucinio bendradarbiavimo, o struktūrinis vienos iš ministerijų padalinys iš esmės nėra pajėgus spręsti tokias problemas. Taip pat, struktūrinis ministerijos padalinys iš esmės negali įtakoti kitų ministerijų resursų panaudojimo bendrai sprendžiant kibernetinio saugumo klausimus.

Be to, be aukščiau paminėtos institucinės sistemos, nustatytos Lietuvos Respublikos kibernetinio saugumo įstatyme, egzistuoja tam tikra fragmentacija ir funkcijų dubliavimas. 2011 m. LR Vyriausybės nutarime dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos patvirtinimo įvardijama daugybė institucijų, atsakingų už kibernetinį saugumą Lietuvoje bei programos įgyvendinimą. Jaučiamas vieningos ir aiškios sistemos trūkumas. Taip pat, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 5 str. 4 d. nurodyta, jog Vidaus reikalų ministerija formuoja politiką valstybės informacinių išteklių saugos srityje tiek, kiek tai neapima kibernetinio saugumo, ir informacinių technologijų taikymo viešojo administravimo (elektroninės valdžios) srityje ir pagal kompetenciją:

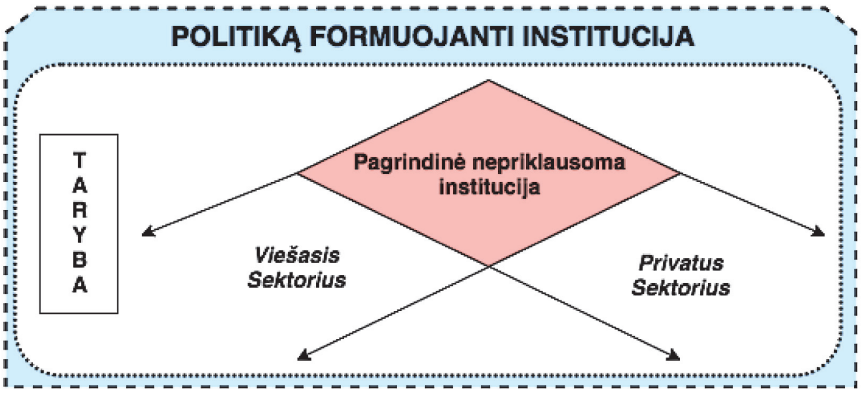
1. organizuoja informacinių technologijų priemonių valdymo ir saugos vertinimą;
2. renka ir analizuoja informaciją apie institucijų valdomų valstybės informacinių išteklių saugą ir tam naudojamas lėšas, teikia Vyriausybei ir institucijoms pasiūlymus dėl valstybės informacinių išteklių saugos ir lėšų valstybės informacinių išteklių saugai poreikio bei efektyvesnio jų naudojimo;
3. rengia informacijos saugos reikalavimus, saugos dokumentų turinio gaires;
4. atlieka saugos reikalavimų laikymosi priežiūrą tiek, kiek tai neapima kibernetinio saugumo;
5. derina su valstybės informacinių sistemų, registro duomenų ir registro informacijos sauga susijusių teisės aktų, saugos dokumentų projektus;
6. derina valstybės informacinių sistemų ir registrų nuostatų projektų nuostatas, susijusias su informacijos sauga;
7. konsultuoja valstybės informacinių sistemų ir registrų valdytojus, valstybės informacinių sistemų ir registrų tvarkytojus, kitas institucijas valstybės informacinių išteklių saugos klausimais;
8. nustato informacijos svarbos įvertinimo, valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo pagal jose apdorojamos informacijos svarbą kriterijus ir jų priskyrimo atitinkamai kategorijai tvarką;

9. atlieka kitas Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatytas funkcijas.

Kaip teigiama Valstybės kontrolės ataskaitoje, trūksta kompetencijos atskyrimo formuojant ir įgyvendinant kibernetinio saugumo ir el. informacijos saugos politiką, neperžiūrėtos vykdomos funkcijos, kurios nebeatitinka pasikeitusio reglamentavimo[45]. Lietuvoje dirbtinai išskirti kibernetinio saugumo ir elektroninės informacijos saugos institutai ir atsakingos institucijos didina administracines sąnaudas, nes dalis funkcijų yra dubliuojama, neaiškus pavaldumas.

Trečia, pagal užsienyje egzistuojančią praktiką, galima teigti, jog galimi keli organizacinės struktūros modeliai. Visgi, labiausiai pasiteisinantis – centralizuoto požiūrio modelis, kai kuriama viena centrinė institucija, kuri turi kompetenciją prižiūrėti visus susijusius sektorius.

Paveikslėlis Nr. 9. *Autorių sudaryta apibendrinta institucinė schema*



Nėra priežasčių šio modelio netaikyti Lietuvoje. Todėl, Lietuvoje turėtų būti įvardijama viena savarankiška, už kibernetinį saugumą atsakinga institucija, atskaitinga Lietuvos Respublikos Vyriausybei. Taip pat, turėtų būti pašalinta už kibernetinį saugumą atsakingų institucijų funkcijų fragmentacija bei funkcijų dubliavimas, ypač kibernetinio saugumo ir elektroninės informacijos saugos srityse.

Pagrindinis principas, nustatant valdymo sistemą: turėtų būti užtikrintas veiklos savarankiškumas bei funkcijų atskyrimas. Funkcijų atskyrimas turėtų pasireikšti politikos formavimo bei kontrolės funkcijų aiškiu atskyrimu.

Išskirtini šie institucijos nepriklausomumo požymiai:

- Institucija, atlikdama savo užduotis, veikia visiškai nepriklausomai;
- Institucija, atlikdami savo užduotis, nepatiria nei tiesioginės, nei netiesioginės išorės įtakos ir neprašo bei nepriima jokių nurodymų;
- institucijai suteikiami žmogiškieji, techniniai ir finansiniai ištekliai, patalpos ir infrastruktūra, kurie yra būtini, kad ji veiksmingai atliktų savo užduotis;
- institucija finansiškai kontroliuojama nedarant poveikio jos nepriklausomumui ir turi atskirą viešą metinį biudžetą.

Lietuvos kibernetinio saugumo strategijoje taip pat turėtų būti aiškiai įvardinta institucija, atsakinga už strategijos įgyvendinimo priežiūrą, koordinavimą, kontrolę bei strategijos atnaujinimą. Tokia funkcija galėtų būti priskirta institucijai, atsakingai už politikos formavimą kibernetinio saugumo srityje.

Taip pat, strategijoje turėtų būti nurodytas įvairių subjektų, dalyvaujančių įgyvendinant strategiją, sąrašas. Nurodant tokį sąrašą, turėtų būti aiškiai išskirtos funkcijos ir atsakomybės.

45 Valstybinio audito ataskaita. Kibernetinio saugumo aplinka Lietuvoje. LR valstybės kontrolė. 2015. Žiūrėta 2016 10 29// www.vkontrole.lt

6. KIBERNETINIS SAUGUMAS NACIONALINĖJE SAUGUMO SISTEMOJE

6.1. Strategijos ryšys su teisės aktais

Būsima Lietuvos Respublikos kibernetinio saugumo strategija turėtų kompleksiškai integruotis šalia aukščiau išdėstytų teisės aktų. Visais minimais dokumentais yra siekiama kuo didesnio Lietuvos Respublikos saugumo, kad kuo geriau būtų užkirstas kelias įprastiems itin svarbios valstybinės reikšmės infrastruktūrų veiklos sutrukdymams ir atakoms elektroninėje erdvėje, o taip pat būtų tinkamai į juos reaguojama. Vis dėlto, galima būtų išskirti, kad dalis aukščiau analizuotų dokumentų kalba apie saugumą plačiąja prasme (LR Konstitucija, 2012 m. Nacionalinė saugumo strategija, 1996 m. LR Nacionalinio saugumo pagrindų įstatymas), o kita dalis labiau specifiškai orientuota į kibernetinį saugumą (ES kibernetinio saugumo strategija, Europos Parlamento ir Tarybos Direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti, LR Kibernetinio saugumo įstatymas, 2011 m. LR Vyriausybės nutarimas dėl elektroninės informacijos saugos (kibernetinio saugumo)). Tokiu būdu manytina, kad būsima Lietuvos kibernetinio saugumo strategija turi būti suderinta su nuostatomis, įtvirtinančiomis saugumą bendrąja prasme ir ypatingai turėtų susiderinti su sąlygomis, kurios jau įtvirtino kibernetinio saugumo reguliavimą Lietuvos Respublikoje.

6.2. Saugumas bendrąja prasme

Nagrinėjant saugumo nuostatas kituose teisės aktuose, galima pastebėti, jog jis atsiskleidžia būtent per suderinamumą su kitais teisės aktais. Pavyzdžiui, 2012 m. Nacionalinio saugumo strategijoje yra nustatoma, kad ši strategija yra grindžiama Lietuvos Respublikos Konstitucija, Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymu (toliau – Nacionalinio saugumo pagrindų įstatymas), Šiaurės Atlanto ir Europos Sąjungos sutartimis. Be to, yra nuorodos ir į kitus tarptautinės teisės aktus: formuodama ir įgyvendindama nacionalinio saugumo politiką, Lietuvos Respublika laikosi visuotinai pripažintų tarptautinės teisės normų, principų ir įsipareigojimų, įtvirtintų Jungtinių Tautų Organizacijos (toliau – JTO), Europos saugumo ir bendradarbiavimo organizacijos (toliau – ESBO) ir Europos Tarybos dokumentuose. Labai panašios, galbūt bendresnės nuostatos dėl saugumo bendrąja prasme turėtų būti įtvirtinamos ir būsimoje kibernetinio saugumo strategijoje. Manytina, kad tokios nuostatos neturėtų būti labai detalios, tačiau atskleidžiančios mintį, jog LR kibernetinio saugumo strategija – dokumentas, turintis ryšį su kitais tarptautinės bei nacionalinės teisės, t.y. LR Konstitucijos, 2012 m. Nacionalinio saugumo strategijos nuostatomis dėl saugumo įtvirtinimo bei vystymo.

6.3. Kibernetinis saugumas

Strategijoje įtvirtinami veiksmai turėtų koreliuoti su veiksmais, apibūdinamais ES kibernetinio saugumo strategijoje, t.y. su veiksmais, kuriais siekiama didinti IT sistemų kibernetinį atsparumą, sumažinti kibernetinių nusikaltimų skaičių ir sustiprinti ES tarptautinę kibernetinio saugumo politiką ir kibernetinę gynybą. Europos Parlamento ir Tarybos Direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių

sistemų saugumo lygiui visoje Sąjungoje užtikrinti iš esmės nustato reikalavimus nacionalinėms valstybių strategijoms, taigi ir Lietuvos Respublikos kibernetinio saugumo strategija turėtų vadovautis esminėmis Direktyvos nuostatomis. Tokiu būdu, Lietuvos Respublikos kibernetinio saugumo strategijoje turi būti apibrėžiami strateginiai tikslai ir tinkamos politikos bei reguliavimo priemonės aukšto lygio tinklų ir informacinių sistemų saugumui pasiekti ir išlaikyti, apimant bent Direktyvoje nurodytus sektorius ir paslaugas.

Ypatingas dėmesys turėtų būti atkreipiamas į būsimos kibernetinio saugumo strategijos suderinamumą su LR kibernetinio saugumo įstatymu, kuris nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžia kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas, valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų ir elektroninės informacijos prieglobos paslaugų teikėjų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones. Strategijoje naudojamos sąvokos, principai galėtų būti suvienodinamos su LR kibernetinio saugumo įstatyme nustatytomis sąvokomis ir principais. Be to, ypač turėtų būti peržiūrima nacionalinė institucinė sistema, atsakinga už kibernetinio saugumo įgyvendinimą. LR Kibernetinio saugumo įstatymo II skyriuje „Kibernetinio saugumo politikos formavimas ir įgyvendinimas“ 4–11 straipsniuose išdėstytos institucijos bei jų įgaliojimai turi atitikti nuostatas, įtvirtinančias kibernetinio saugumo įgyvendinimą strategijoje. Autorių nuomone, siekiant veiksmingesnio kibernetinio saugumo įgyvendinimo, strategijoje turėtų būti apibrėžiama viena institucija, kuri būtų nurodoma kaip atsakinga už kibernetinio saugumo politikos įgyvendinimą ir kontrolę.

Turint omenyje tai, jog LR kibernetinio saugumo strategija – teisės aktas / planavimo strateginis dokumentas, nustatantis kibernetinio saugumo gaires ir tendencijas, jame turėtų būti atskleidžiami tik esminiai reguliavimo dalykai, konkrečias detales bei aspektus paliekant kitiems teisės aktams. Vis dėlto, nepaisant to, kad LR kibernetinio saugumo strategija turėtų būti labiau abstraktaus ir bendresnio pobūdžio dokumentas, jo nuostatos turi neprieštarauti net ir poįstatyminiams teisės aktams, kaip pavyzdžiui, dar galiojančiam 2011 m. LR Vyriausybės nutarimui dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos patvirtinimo, 2013 m. liepos 24 d. Vyriausybės nutarimui dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo, saugos dokumentų turinio gairių aprašo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo. Pastarajame nutarime yra įtvirtintos tokios sąvokos, kaip elektroninės informacijos saugos politika, elektroninės informacijos sauga, konfidencialumas, vientisumas. Jeigu LR kibernetinio saugumo strategijoje bus kalbama apie elektroninės informacijos saugą, saugos incidentus, informacinės sistemos pokyčių valdymą, turėtų būti atsižvelgiama į Vyriausybės nutarime[46] patvirtintas nuostatas.

Autorių nuomone, nagrinėjamas būsimos LR kibernetinio saugumo strategijos ryšys su kitais galiojančiais teisės aktais yra reikšmingas, nes būtent per šį ryšį yra atskleidžiama būsimos strategijos nuostatų svarba. Apibendrinant galima teigti, jog tik visapusiškai ir tinkamai išanalizavus šiuo metu galiojančio reguliavimo sąlygas, pradedant nuo globalią bendruomenę jungiančių tarptautinės teisės nuostatų ir baigiant poįstatyminiais teisės aktais, bus galima sukurti tinkamas nacionalinės LR kibernetinio saugumo strategijos sąlygas.

46 2013 m. liepos 24 d. Vyriausybės nutarimas Nr. 716 „Dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo, saugos dokumentų turinio gairių aprašo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.FC952AC6A109

7. MODELIO NAUDOJIMO GAIRĖS IR TYRIMO RIBOTUMAI

7.1. Modelio naudojimo gairės

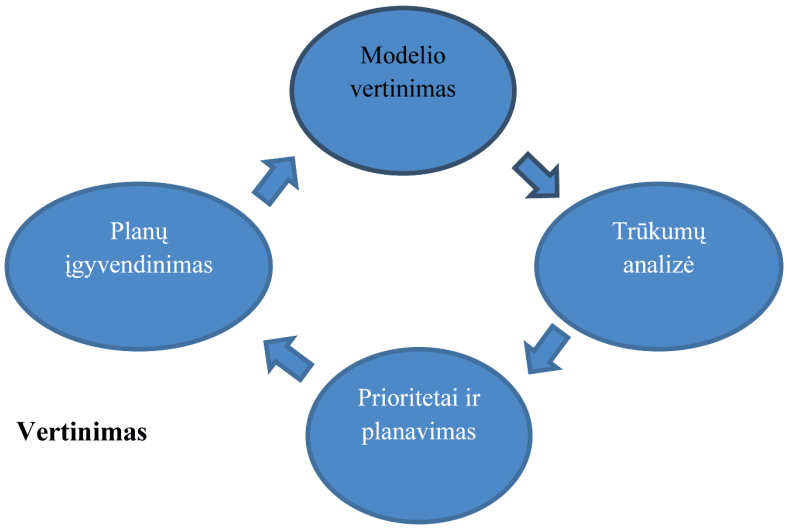
Lietuvos kibernetinio saugumo strategijos modelis skirtas sistemiškai išdiskutuoti tarp suinteresuotų visuomenės grupių ir atsakingų institucijų, įvertinti ir sukurti Lietuvos kibernetinio saugumo strategijai, jai nuolat tobulinti. Kuriant strategiją modelis gali būti naudojamas kaip moksliniais metodais pagrįsta priemonė, kurioje sukauptos naujausios atitinkamos srities žinios, atlikti moksliniai tyrimai bei ištirta geriausia NATO ir ES šalių praktika. Modelis yra priemonė tinkamai strategijai sukurti.

Modelio naudojimo gaires sudarantys žingsniai turėtų būti šie:

1. Inicijuojama darbo grupė.
2. Įvertinamas pateiktas modelis.
3. Modelio pagalba atliekami gilesni tyrimai (analizė atskirų sričių).
4. Įvertinami rezultatai.
5. Konstruojamas tekstas.
6. Diskutuojamas ir derinamas su atitinkamomis visuomenės grupėmis ir organizacijomis.
7. Patvirtinama strategija.

Kadangi kibernetinio saugumo sritis itin dinamiška, viena iš pagrindinių modelio naudojimo gairių – nuolatinis procesų peržiūrėjimas pagal kibernetinio saugumo strategijos tikslus ir pagrindines veiksmų sritis. Kibernetinio saugumo strategija – dinamiškas dokumentas, kuris turi būti adaptuotas pagal aktualias realijas. Vertinant pateiktą modelį galėtų būti naudojama schema, pavaizduota Lentelėje Nr. 2. Už modelio įgyvendinimą turėtų būti atsakinga **<u>viena</u> pagrindinė institucija**. Kitos susijusios institucijos, kurių gali būti daug – labiau prisidedančios/įgyvendinančios institucijos, veikiančios pagal pagrindinės institucijos nurodymus.

Paveikslėlis Nr. 10 *Autorių sudaryta modelio vertinimo schema*



Turinti teisę inicijuoti Lietuvos kibernetinio saugumo strategijos sukūrimą institucija turi suformuoti ekspertų ir institucijų darbo grupę, kuri, pasitelkdama modelį, kurtų strategiją.

Pagrindinis tinkamos strategijos sukūrimo veiksnys yra tinkamas aplinkos analizės atlikimas. Atsižvelgiant į analizės metu nustatytas aplinkybes: šalies ir veiksnių specifiką, trūkumus ir kt., formuluojami tikslai, uždaviniai, principai ir kitos strategijos dedamosios. Kadangi veiksmai, susiję su kibernetiniu saugumu Lietuvos Respublikoje jau yra pradėti įgyvendinti, vertinimo etapas yra ypatingai svarbus. Be to, vertinimas padeda išgryninti esamos situacijos neatitikimus, trūkumus ir / ar klausimus.

Trūkumų analizė

Vertinimo procese išgryninus esamos situacijos (kiek tai susiję su galiojančia kibernetinio saugumo strategija) trūkumus, turi būti sprendžiama, ar minėti trūkumai yra reikšmingi ir kuriuos trūkumus kuri organizacija turėtų spręsti prioriteto tvarka. Nėra būtina spręsti visų trūkumų iš karto. Siektina, jog būtų nustatyti prioritetai pagal kibernetinio saugumo strategijos tikslus ir pagrindines veiksmų sritis ir būtų nustatomi kiekvienos susijusios organizacijos pajėgumai pagal kibernetinio saugumo strategiją. Tokiu būdu kiekviena susijusi organizacija ir jos veiksmai bus suderinti su Lietuvos kibernetinio saugumo strategijos modeliu. Kiekvienoje iš susijusių institucijų taip pat gali būti suformuota darbo grupė, kuri spręstų su trūkumų analize susijusius klausimus.

Prioritetai ir planavimas

Kai įvykdoma trūkumų analizė, pagrindinė organizacija turėtų nustatyti prioritetus konkretiems veiksmams. Be to, šiame etape taip pat turi būti nustatomas planas, pagal kurį turi būti šalinami nustatyti neatitikimai ir trūkumai. Tokie planai gali apimti skirtingus laikotarpius, priklausomai nuo siekiamo rezultato ar siektinų kibernetinio saugumo pajėgumų sustiprinimo.

Planų įgyvendinimas ir nuolatinė peržiūra

Ankstesniame skyrelyje minimi planai turėtų būti įgyvendinami tam, kad būtų pašalinami nustatyti neatitikimai bei trūkumai. Modelio vertinimas yra ypatingai susijęs su įgyvendinimo dalimi ir turėtų būti nuolatos atliekamas dėl siektinų rezultatų. Ypatingais atvejais gali būti įtraukiami pakartotiniai vertinimai tam, kad būtų suvaldoma itin greitų pokyčių rizika kibernetinio saugumo srityje.

Rekomenduojamas Lietuvos kibernetinio saugumo strategijos modelio naudojimo gairių procesas pagrindinei institucijai bei kitoms susijusioms institucijoms pateikiamas Lentelėje Nr. 2.

Lentelė Nr. 2. *Autorių sudarytas rekomenduojamas Lietuvos kibernetinio saugumo strategijos modelio naudojimo gairių procesas*

	Veiksmai ➡	**Rezultatas**
Modelio vertinimas ⬇	1. Vertinimo atlikimas	Vertinimo ataskaita
Trūkumų analizė ⬇	1. Trūkumų analizė 2. Potencialių pasekmių, kylančių dėl trūkumų, analizė 3. Prioritetinių trūkumų nustatymas	1. Trūkumų bei jų pasekmių sąrašas
Prioritetai ir planavimas ⬇	1. Būtini veiksmai trūkumams pašalinti 2. Būtinos lėšos (jei taikoma) 3. Nustatyti veiksmų prioritetai 4. Planas prioritetų įgyvendinimui	1. Planas su nustatytais įgyvendinimo prioritetais
Planų įgyvendinimas ir nuolatinė peržiūra	1. Plano priežiūra 2. Plano nuolatinė peržiūra	1. Duomenys dėl plano priežiūros

Vertinant parengtą modelį, turi būti įvertinamos kibernetinės rizikos, tiek vidinės, tiek išorinės. Turi būti vertinami sektoriai, išskirti šiame modelyje aukščiau, t.y. privatus ir viešasis sektorius. Taip pat, turėtų būti atliekami tyrimai dėl kibernetinės kultūros, tikslu nustatyti kibernetinės kultūros Lietuvoje lygį. Tyrimai dėl kibernetinės kultūros turėtų apimti visas galimas sritis. Tik atlikus tokius tyrimus, kai žinomas atspirties taškas, galima planuoti kibernetinės kultūros kėlimą Lietuvoje.

Parengtas modelis taip pat gali būti taikomas jau turimo kibernetinio saugumo strategijos projekto vertinimui.

7.2. Tyrimo apribojimai

Rengiant kibernetinio saugumo strategijų modelį buvo tirtos autorių pasirinktos 1 modelio dalyje nurodytos ES ir NATO valstybių strategijos. ES ir NATO nacionalinių valstybių kibernetinio saugumo strategijų palyginimas buvo atliekamas lyginant pagrindinius kriterijus, kuriuos patys autoriai išskyrė kaip pagrindinius. Šiame modelyje buvo analizuoti kibernetinio saugumo strategijų 1) principai, 2) bendradarbiavimas su privačiu sektoriumi, 3) kova su elektroniniais nusikaltimais, 4) kibernetinė gynyba, 5) moksliniai tyrimai, 6) standartai, 7) pagrindinių vertybių rėmimas, 8) „žaidėjų“ / institucijų užduotys bei kompetencija.

Reikia atkreipti dėmesį, kad kibernetinis saugumas – tarptautinė sritis. Viena vertus autoriams buvo pakankamai sudėtinga analizuoti kitų valstybių parengtas kibernetinio saugumo strategijas dėl kultūrinių skirtumų, valstybių dydžio, skirtingos geopolitinės bei ekonominės padėties. Kita vertus, daugelis dokumentų buvo analizuojami arba anglų kalba, todėl tyrimas yra apribojamas autorių anglų kalbų žinių lygiu arba atliktais vertimais. Kai kurios strategijos (tik kelios) buvo surašytos nacionaline kalba, be vertimo į anglų kalbą, tad autoriams teko naudotis „google translator“ funkcija, todėl tekste galėjo atsirasti netikslumų.

Aukščiau išvardinti tyrimo apribojimai nesumažino atlikto tyrimo mokslinės vertės ir neturėjo esminės reikšmės tyrimo rezultatams. Tačiau minėti tyrimo apribojimai atkleidė tolimesnius galimus tęstinius tokio projekto darbus. Autoriai nustatė, kad tolesniam tiriamojo objekto pažinimui reikėtų tirti atitinkamai visų ES ir NATO valstybių pilną teisinę ir susijusią aplinką (o ne tik kibernetinio saugumo strategijas), pvz., nacionalinio saugumo strategijas, įvairius valstybių vystymosi planus ir pan. Tai galėtų padėti geriau atskleisti kibernetinio saugumo strategijų kaip dokumentų vietą nacionalinėje sistemoje, taip pat ryšį su nacionaliniu saugumu atitinkamose valstybėse. Dėl per didelės (ir finansuojamo projekto apimtis bei planus viršijančios) darbų apimties bei trumpų terminų į šio modelio nagrinėjimą šie veiksmai nebuvo atlikti.

NAUDOTA LITERATŪRA*

* Šį literatūros sąrašą sudaro tik informacija, papildomai naudota rengiant Lietuvos kibernetinio saugumo strategijos modelį. Atkreiptinas dėmesys, kad vykdant projektą „ES ir NATO valstybių kibernetinio saugumo strategijų normų analizė ir adaptavimas Lietuvos situacijai – Lietuvos kibernetinio saugumo strategijos modelis bei rengiant straipsnius buvo naudota ir kita literatūra, kuri nėra nurodoma šiame sąraše. Išsamus tokios literatūros sąrašas pateikiamas publikuotų straipsnių literatūros sąrašuose.

1. An evaluation framework for Cyber Security Strategies, ENISA, 2014. Žiūrėta 2017 01 17 // https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1
2. Breaking news from the FTTH Conference 2016: Croatia, germany and Poland join the FTTH ranking. Fibre to the home conference "Calling for a brigher future", Council Europe, 2016. Žiūrėta 2016 06 20 // http://www.ftthcouncil.eu/documents/PressReleases/2016/PR20160217_FTTHranking_panorama_award.pdf
3. 2016 m. II ketvirčio CERT-LT veiklos ataskaita, CERT-LT, 2016. Žiūrėta 2016 09 28 // https://www.cert.lt/doc/2016_2.pdf
4. Digital Single Market. Country profile for Lithuania, eGovernment indicators. European Commission, 2017. Žiūrėta 2017 03 02 // https://digital-agenda-data.eu/charts/country-profiles-the-relative-position-against-all-other-european-countries#chart={%22indicator-group%22:%22egovernment%22,%22ref-area%22:%22LT%22,%22time-period%22:%222015%22}
5. ES kibernetinio saugumo strategija. 2013. Prieiga per internetą: http://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52013JC0001&from=LT
6. Europos Parlamento ir Tarybos Direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. 2016. Prieiga per internetą: .
7. Europos Parlamento ir Tarybos Direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR. 2013. Prieiga per internetą: http://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32013L0040&from=LT.
8. ENISA NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies. 2016. Prieiga per internetą: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.
9. EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace, BSA, 2015. Žiūrėta 2017 01 17 // http://cybersecurity.bsa.org/index.html
10. Fibre to the home conference "Calling for a brigher future", Council Europe, 2016. Žiūrėta 2016 06 20 // http://www.ftthconference.eu/images/Banners/Conference2016/Media%20downloads/20160217PressConference_presentation.pdf
11. Grėsmių nacionaliniam saugumui vertinimas. Lietuvos Respublikos Valstybės saugumo departamentas ir antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos, Vilnius, 2016. Žiūrėta 2016 09 26// http://www.vsd.lt/Files/Documents/635948635773762500.pdf.
12. Išankstinio tyrimo ataskaita. Strateginės informacijos sauga. LR valstybės kontrolė. 2009. Žiūrėta 2016 10 29// www.vkontrole.lt.

13. ITU NATIONAL cybersecurity guide. International telecommunication union. 2011. P. 13. Žiūrėta 2016 10 29//http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
14. Įvertinimo ataskaita apie Lietuvą. Septintasis tarpusavio vertinimo etapas „Europos kibernetinių nusikaltimų prevencijos ir kovos su tokiais nusikaltimais politikos praktinis įgyvendinimas ir veikimas“. ES Taryba. Briuselis, 2016. Žiūrėta 2016 11 10 // http://data.consilium.europa.eu/doc/document/ST-6520-2016-REV-1-DCL-1/lt/pdf
15. Lietuvos gyventojų mokėjimo įpročių apklausos apžvalga, Lietuvos bankas, 2015. Žiūrėta 2017 02 11// https://www.lb.lt/lietuvos_gyventoju_mokejimo_iprociu_apklausos_apzvalga_2015_m
16. Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės siūlymu šioje strategijoje turės būti apibrėžti ir ypatingos svarbos informacinės infrastruktūros nacionaliniu mastu apsaugos principai.
17. LR valstybės informacinių išteklių valdymo įstatymo projektas, LR Seimas, 2016. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/d0515db0afba11e68987e8320e9a5185?jfwid=-wd7z8bvie
18. Nutarimo dėl LR Seimo 2002 m. gegužės 28 d. nutarimo Nr. IX-907 „Dėl nacionalinio saugumo strategijos patvirtinimo“ pakeitimo projektas, LR Seimas, 2016. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/407015b094f311e68adcda1bb2f432d1?jfwid=-wd7z8nw39
19. Nutarimas dėl LR Seimo 2002 m. gegužės 28 d. nutarimo Nr. IX-907 „Dėl nacionalinio saugumo strategijos patvirtinimo“ pakeitimo, LR Seimas, 2016. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/2c6e04b0e30811e68503b67e3b82e8bd
20. Prezidentė Dalia Grybauskaitė: informacinė apsauga turi būti vykdoma operatyviai ir koordinuotai. Interneto dienraštis 15min.lt. 2016. Žiūrėta 2017 02 15. http://www.15min.lt/naujiena/aktualu/lietuva/dalia-grybauskaite-informacine-apsauga-turi-buti-vykdoma-operatyviai-ir-koordinuotai-56-341758
21. Ritchie J. ir Lewis J. *Qualitative Research Practice: A Guide for Social Science Students and Researchers.* Sage, 2003.
22. Ryšių reguliavimo tarnybos 2016 06 30 LR Elektroninio parašo įstatymo įgyvendinimo 2015 metų ataskaita, Ryšių reguliavimo tarnyba, 2016. Žiūrėta 2017 01 20 // http://www.rrt.lt/lt/apzvalgos-ir-ataskaitos/elektroninio-paraso-istatymo-1b73.html
23. Seidmen I. *Interviewing as Qualitative Research: A Guide for Researchers in Education and Social sciences*. Teachers College, Columbia University, New York and London, Forth edition. 2005.
24. Štitilis D., Paškauskas Ž., „Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė,“ *Jurisprudencija* 2 (92), 2007: 37–45. Žiūrėta 2016 08 15//https://www.mruni.eu/en/mokslo_darbai/jurisprudencija/archyvas/dwn.php?id=267948
25. Valstybinio audito ataskaita. Kibernetinio saugumo aplinka Lietuvoje. LR valstybės kontrolė. 2015. Žiūrėta 2016 10 29// www.vkontrole.lt
26. 2013 m. liepos 24 d. Vyriausybės nutarimas Nr. 716 „Dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo, saugos dokumentų turinio gairių aprašo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.FC952AC6A109

PRIEDAI

Priedas Nr. 1. Užsienio ekspertų aprašymas

Samantha Adams (Nyderlandų Karalystė) – Tilburgo universiteto (angl.– University of Tilburg, Nyderlandų karalystė) Tilburgo teisės, technologijų ir visuomenės instituto (angl. TILT- Tilburg institute for law, technology and society), asocijuota profesorė. Pagrindinės mokslinių tyrimų sritys yra susijusios su informacinių technologijų ir sveikų praktikų santykio analize. Kitos tyrimų kryptys apima technologijų normatyvus, besikeičiančius apibrėžimus tarp ligų ir sveikatos, socialinių tinklų naudojimą teikiant centralizuotą medicininę pagalbą ir kokybinių tyrimų metodus tiriant minėtas sritis.

Lorenzo Dalla Corte (Italija) – Delft technologijų universiteto (angl. – Delft university of technology, trumpinys – TU Delft) mokslinis bendradarbis, dirbantis su duomenų apsaugos projektais. Be to, Lorenzo Dalla Corte buvo ir Tilburgo universiteto (angl. – University of Tilburg, Nyderlandų karalystė) Tilburgo teisės, technologijų ir visuomenės instituto (angl. TILT – Tilburg institute for law, technology and society) tyrėjas.

Sintija Deruma (Latvijos Respublika) – BA School of Business and Finance, MBA studijų kibernetinio saugumo valdymo programos vadovė ir mokslinė bendradarbė. UAB „Latvia's State Forests" kibernentinio saugumo vadovė, konsultantė asmens duomenų teisinės apsaugos klausimais.

Uldis Kinis (Latvijos Respublika) – Latvijos Konstitucinio teismo teisėjas, Stradins University Riga teisės profesorius. Pagrindinės tyrimų kryptys: teisinė informatika, informacinių technologijų teisė, kibernetinis saugumas, elektroniniai nusikaltimai.

Jesus Maria Gonzalez Perez (Ispanija) – kibernetinio saugumo vadovas SYNEIDIS Cybersecurity organizacijoje, buvęs kariuomenės kibernetinio saugumo vadovas. Jesus Maria Gonzalez Perez taip pat dalyvavo įvairiose ES ir Jungtinių tautų misijose.

Anna Sarri (Graikija) – Europos tinklų ir informacijos saugumo agentūros (angl. – ENISA) tinklų ir informacijos saugumo pareigūnė. Geryjų praktikų, gairių ir rekomendacijų, susijusių su kibernetinio saugumo strategijų valdymu, teikimas – viena iš pagrindinių Anna Sarri veiklos krypčių.

Dimitra Liveri (Graikija) – Europos tinklų ir informacijos saugumo agentūros (angl. – ENISA) ekspertė. Geryjų praktikų, gairių ir rekomendacijų, susijusių su kibernetinio saugumo strategijomis, privačiu ir viešu bendradarbiavimu, teikimas, kibernetinio saugumo praktiniai užsiėmimai – viena iš pagrindinių Dimitra Liveri veiklos krypčių. Dimitrs Liveri dirba padedant valstybėms narėms įgyvendinti nuotolinės kompiuterijos paslaugas viešuosiuose pirkimuose. Be to, Dimitra Liveri padeda įgyvendinti kibernetinio saugumo strategijas nacionaliniu lygmeniu patariant, kaip valstybės narės gali pagerinti savo tinklų ir informacijos saugumą.

Johan Stronkhorst (Belgija) – vyresnysis saugumo analitikas KBC Bank & Verzekering. Be to, Johan Stronkhorst yra vyresnysis vadovybės konsultantas IT saugumo ir rizikų valdyme, verslo procesuose ir (finansinėse) administracinėse sistemose (ERP). Konsultuoja įvairias bendroves saugumo plataus spektro saugumo klausimais.

Jaan Priisalu (Estija) – Talino technologijų universiteto tyrėjas. Pagrindinės tyrimų kryptys: kibernetinis saugumas, IT rizikų valdymas. Jaan Priisalu turi IT ir rizikų valdymo vadovaujamosios patirties korporatyvinėse organizacijose (Swedbank). Be to, Jaan Priisalu 3 metus dirbo Estijos informacinių sistemų insituticijos vadovu.

Ferenc Szalai (Vengrija) – Vengrijos atstovas NATO jungtiniame kibernetinės gynybos kompetencijų centre (angl. – Cooperative Cyber Defence Centre of Excellence, trumpinys – NATO CCDCOE), švietimo ir pratybų grupėje.

Kadri Kaska (Estija) – vyresnioji analitikė NATO jungtinio kibernetinės gynybos kompetencijų centre (angl. – Cooperative Cyber Defence Centre of Excellence, trumpinys – NATO CCDCOE), įsikūrusiame Taline, Estijoje. Kadri Kaska dirbo teisės patarėja nacionalinėje ryšių reguliavimo tarnyboje, dalyvavo rengiant pagrindinius nacionalinius teisės aktus bei patariant ryšių valdymo ir konkurencijos klausimais. Nuo 2008 m. Kadri Kaska dirba jungtiniame kibernetinės gynybos kompetencijų centre, ji specializuojasi informavimo ir komunikavimo teisės klausimais, elektroninių nusikaltimų ir kibernetinio saugumo aspektais nacionalinio saugumo įstatymo kontekste klausimais. Dabartinės Kadri Kaska pagrindinės tyrimų kryptys apima nacionalinių kibernetinio saugumo strategijų analizę, o taip pat ir organizacinius kibernetinio saugumo modelius.

Priedas Nr. 2. Klausimai užsienio ekspertams ir užsienio ekspertų atsakymai*

* Ekspertų atsakymų eiliškumas neatskleidžia ekspertų eiliškumo ekspertų sąraše aukščiau.

1. Is it important to have a national cybersecurity strategy? Please argue your answer.(10 responses)

It is increasingly important for governments to be prepared to deal with external attacks on critical systems and thus, yes, to have a formal strategy for securing cyber structures and environments at the national level.

Yes, cyber warfare is a paramount modern warfare domain, and cybercrime is naturally on the rise.

yes, strategy is a clear vision and strategic goals as well as detailed measures, terms and responsible entities for achieving the goals

Absolutely. Cyber security strategy of course is not a law, but it precisely indicates problems and solutions, what state should have to take into account for creating safe and secure electronic environment.

Yes indeed. NCSS defines the governance framework for cyber security and it is certainly the most important part of the whole process of cyber security to protect information or infrastructures. Modern life depends upon the timely, adequate and confidential performance of cyberspace. Since governments mainly exist to maintain social order, protect the lives and property of their citizens and enable commerce, then national leaders are accountable for cybersecurity as it supports all the aforementioned services. Cybersecurity is a national policy matter because the illicit use of cyberspace could hamper economic, public health, safety and national security activities. Thus NCS strategies are important to all States because it endeavours to ensure that cyberspace continues to work when and as expected even under attack. Governments must use all instruments of national power to reduce cyber risks appropriately. In particular, national leaders have accountability for devising a cybersecurity strategy and fostering local, national and global cross-sector cooperation.

Yes it is important. A national cyber security strategy is a tool to improve the security and resilience of national information infrastructures and services. It is a high-level, top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. As such, it provides a strategic framework for a nation's approach to cyber security.

It is essential, regarding the cyberthreats facing the national cybersecurity.

Ressources are always scarce. Strategy should give priorities and align efforts of different actors in the society towards common goals. It provides basis for effectiveness and efficiency.

It is important to have a wildly agreed and accepted document that states the threats and challenges, that the certain country faces and the long term agreed vision how to face the challenges.

Definitely. The need for a national cyber security strategy (NCSS) derives from the variety of different actors who determine the national cyber security posture – different government agencies and private sector service providers. A comprehensive national cyber security strategy (NCSS) is instrumental to ensuring coherence and consistency in their actions; without a defined NCSS, there is a very clear risk of conflicting objectives, varied levels of ambition, and waste of resources.

2. What is the relation between national cyber security strategy and other state`s documents (including legal acts)? (10 responses)

I'm not sure I understand the question.

It depends from the nation concretely considered. I'd assume most CSSs have the status of programmatic documents, but I'm not sure.

the implementation of the strategy be enshrined in respective laws and subordinate legislation

Firstly cybercrime strategy is a planning and vision document. Secondly: During preparation phase, experts conduct profound analysis of existing legal acts: thirdly this analysis disclose also existing drawbacks for existing regulations.

To outline and define necessary policy and regulatory measures and clearly defined roles, responsibilities and rights of the private and public sector (e.g. new legal framework for fighting cybercrime, mandatory reporting of incidents, minimum security measures and guidelines, new procurement rules, identify critical infrastructures (CIIs) including key assets, services and interdependencies, response and recovery plans and measures for protecting such CIIs, organizational structures that develop, implement and test these preparedness, response and recovery plans and measures). For example, the strategy from Slovakia identifies a need to define a legal framework for the protection of cyberspace. In several strategies there is a particular focus on cybercrime. For example in The Netherlands which aims to intensify investigation and prosecution of cybercrime. France also stresses this point and wish to promote the strengthening of current legislation and international judicial cooperation.

Cyber security strategy need to take into account already existing and implemented regulations but also should be the incentive to create new regulations if needed.

Documents on privacy, telecom, critical network infrastructure.

Strategy provides vision. Legal acts are fixing agreed status quo. legal acts are means to achieve goals set in the strategy.

Usually the strategy is built uppon the national defence strategy and in line with other national strategies (development, foreign affairs, economic strategies).

There is a clear link between a NCSS and domestic security/national security/defence strategy, and a NCSS and an ICT/information society strategy. The NCSS objectives of these should ideally be consistent and realistically at least not conflicting. Consistency between the NCSS and other national strategies may need to be considered as well (e.g. strategies for critical information system-dependent sectors such as energy supply; crime and terrorism prevention, crisis management). As for strategy vs law, the same distinction applies as between national strategy and national law in any domain, there is nothing specific about cyber in particular. A national strategy defines the state's political vision and overall objectives in a certain area, and describes the measures necessary to attain these objectives. A legal act is an instrument that implements these measures, especially as it comes to affecting the rights and obligations of persons.

3. Do you think that the national cyber security strategy should be a document formulating a vision, strategic goals and other strategic issues, or a detailed document establishing a vision and strategic goals as well as detailed measures, terms and responsible entities for achieving the goals, laying down functions of institutions, etc.? Please explain your opinion.(10 responses)

I believe it should incorporate both strategic goals and options for how to reach those. Detailed measures are good but should allow for flexible response. I also believe that in a possible crisis situation that there should be clarity regarding who is primarily responsible and what the chain of command is, which is reinforced if functions are clear prior to any sort of incident.

I'd see a national CSS to be a high-level document, formulating a general strategy to be concretely implemented on a case by case basis.

2nd approach is more practical way to achieve real change

Sure. Strategy as a vision and planning document, should include all characteristics included into question. However strategy it self does not create any rights and obligations to stakeholders. It is worth to say that according to goals mentioned in cyberstrategy, legislator and experts, shall plan further development of statutory regulations concerning all stakeholders.

In my view the NCSS must be a comprehensive, flexible, dynamic and living document, in order to easily meet new and global threats, and to improve and enhance the use of information and communication technologies for government, industry and citizens. On the other hand NCSS should also address in detail responsibilities, goals and functions of public and private stakeholders (governmental departments, national regulatory authorities, public bodies, armed forces, industry, academia, citizen representatives, etc); avoiding duplication of efforts.

Developing a comprehensive strategy can pose many challenges. A document that ticks all the right boxes for what should be included can be easily made. However, this is unlikely to achieve any real impact in terms of improving the cyber security and resilience of a country. The content of the final document depends on the priorities and the vision of the country.

Since detailes measures will be outdated in a very short time, the main goals are the most important. terms and entities can be stable elements, but detailes measures are never sustainable on a longer term. The annexes, renewed every year, might detail those measures and react on upcoming cyber threats.

Strategy should define goals and priorities. Implementation plan should be separate document stating how those goals will be met. The plan would change more often during the development – environment changes and people become more knowledgeable and would be wiser in choosing the ways of implementation.

I think the strategy should identify the existing baseline to build upon, including the analysis of threats challenges the country facing, and the prioritisation of these threats. Than the vision can be explained. The detailed action program , with performance indicators, responsible entities and allocated resources can be put in the strategy, in action program, in acts. I think in line with the strategy decision the nation should approve the action items with the responsible authorities with allocated resources.

The NCSS as a strategic document should define a mid-term vision (practice points to the NCSS litetime to be between 3–5 years, which seems to be a feasible length). The detailed measures, terms, and entities bearing responsibility for implementation need to be defined in order to successfully implement the NCSS, but predicting a detailed future roadmap for the entire lifespan of a NCSS is unlikely to be very successful. Implementation might be best addressed in shorter phases (e.g. 2-year implementation plan, then review and possible corrections).

4. Which cyber space elements (solely the internet or the intranet as well, other devices unconnected to the internet) should the issues provided for in the strategy cover? (10 responses)

Increasingly, „unconnected" devices are becoming connected and therefore it is good to develop a strategy that covers both.

I'd argue that it should cover networks, information and infrastructure as a whole. No point leaving possible attack vectors out.

people, process, technology

Cybersecurity shall be considered a a broad concept. This concept include all elements of information system security. Moreover it means that it should include, IT objects, terrestrial objects, networks etc.

I consider important that NCSS be focused on the right risks and involvement of all stakeholders. Thus, internet, intranet and unconnected networks should be covered.

a cyber security strategy should include provisions for infrastructures critical for the society. For example, critical information infrastructure protection, cyber defence, awareness raising, information sharing, capability building, incident reponse, etc.

The so called smart grids related to the critical infrastructure are the most important. Usually this is energy and telecom related. But it is also a part of the industry and, for example, important infrastructures like ports and airports.

Cybersecurity is not computer security. You should protect all information systems supporting critical processes in the society disregarding their location, zone or territory. But you should also protect trust, isntitutions and communication between them.

not understand the question

The key word is „cyberspace" – if the systems/devices can (even potentially) connect to a common digital space, regardless of the extent of such space, they should be included in the scope of the NCSS, regardless of whether such connection is permanent, temporary, or local. Then, the measures intended for different kinds of systems may well be different: a local network may expectably not face the same security requirements as vital national infrastructure etc.

5. What, in your opinion, should be the validity period of the national cyber security strategy?(10 responses)

Both short and long term, to allow for concrete plans now but also flexibility to adjust to changes in technology that could be relevant to cyber security.

Two years, with a review after 6 month/ 1 year

3–5

In my opinion, strategy should not be valid more than 4–5 year period. Apart from this I think that document should consist by part, which describes general principles of whole process. Secondly – proposed activities and tasks to be done. Second part shall be subject for yearly updating process.

Although being a living document, a four years validity period seems appropriate

2–5 years.

Strategy perhaps 5 years, but with an annual review and update.

In quick changes it should be reviewed in two years (like did Netherlands) in normal situation four years. However, some goals should be set in 10 years, so the strategies will have overlap and continuity.

The strategy can cover short and long therm goals. I think 2–3 year provides enough flexibility and continuity.

3 to 5 years.

6. Why do you think national cyber security strategies are so different? What are the criteria/ reasons that have led to such a diversity of strategies (even strategies of very similar countries differ significantly)?(10 responses)

I think it has grown that way and is attributable to how they run the affairs of state. Some countries place economic ministries in the lead, others communications and still others defense, but this is from out the reasoned logic of how their country works. I also think it has to do with awareness and the sense of (perceived) urgency that each state has.

Different states with different needs and different legislations implementing CSSs at different moments in time and with different aims, probably. I'd imagine it's because of the same reasons why e.g. military strategies differ from country to country – too many things differ from country to country to have a uniform approach.

the knowledge, skills, abilities of political creators, decision makers, security budget,national capabilities

1. Cyber security strategy is inseparable with legislative system of national country. Each such system is unique. It means that national legislative system based on national traditions, legal culture and consciousness.

Nations have different national capabilities, needs, threats, values, culture and interests; these influence the perception of risk and thus their cybersecurity strategy. The understanding of cyber security and other key terms varies considerably from country to country, and influences the different approaches to cyber security strategy. Moreover cybersecurity strategies often flow from the national security strategy. For example, the national security strategies of Canada, the UK and the USA name cyber attacks as priority risks. States may issue a defence cybersecurity strategy to enable military and intelligence operations.

It depends on cultural differences and on the priorities and the maturity of the country.

This is a very negative effect of the political nature of everything related to national (cyber) security.

Goal is to protect processes in the society. Awareness, understanding, culture, economy and important processes in the society are different. Interests might be similar but every ecosystem is different.

Nations have different awareness level, different baseline and most importantly different goals. Some would focus on building economy, others are the militarisation of cyber or usage for intelligence.

Organisational setup, political and legal culture, political priorities (e.g. emphasis on sovereignty, economic benefit, or information society development), national experience from major cyber incidents, and last but not least, human factors related to personalities of key officials. That being said, the forms of NCSS are often more diverse than the actual contents.

7. What are the areas where the context of the national cyber security strategy could manifest? (10 responses)

I don't understand this question – is this asking for sectors or

Law enforcement, intelligence, warfare, information assurance... I am not sure whether I fully understand this question, however

cybercrime prevention, critical infrastructure protections, security professionals education not awareness, mandatory controls, risk management as approach, as the instrument

Obligation to bound with international principles of law, protection of human rights shall enshrined as a treasure. It also would be relevant that strategy would include also principles and functions how state should act for achieving goals.

Government, international partners and the private sector: Economy: Protecting Networks: Enhancing Security, Reliability, and Resiliency. Military. Internet. Critical infrastructure protection. Standards, norms and legislation Collaboration between authorities, business and academician Culture of security: inform, educate and raise awareness. Research, development and innovation. Counter national and international criminal activities. Threat tracking, risk assessment and response.

establish and implement a legislative framework, establish and clarify roles and collaboration between the public and private sector, invest in ICT and innovation for cybersecurity and privacy, critical information infrastructures protection, data protection, protect digital national information resources, education and training, international collaboration, prepardness and response against cyber threats and attacks, promote economy reliant digitalised industry, awareness raising, tackle cybercrime, democracy and respect of human fundamental rights

This should be related to data protection, critical infrastructure and privacy. Other subjects, like cybercrime, technical measures, internet, should be on a transnational (e.g. EU) level harmonized.

Economy, state defence, internal security, information souveranity, legal institutions and their relations (in broader sense copperation of communities), education and research.

CIP, cooperation: international, academia, private-public, incident detection, response, cyber crime, child protection, knowledge and skill development. Management of cyber activities.

(not sure I understand the question)

8. Ideally, what are the elements/ aspects which should be emphasized as the most important in the national cyber security strategy? Please itemize them. (10 responses)

Guarding critical infrastructures, learning from other countries and good communication

1. Critical infrastructure protection 2. Information Assurance 3. Signals intelligence 4. Public/private cooperation 5 CERT/CSIRT role within the nation's infosec ecosystem

short terms fixes and long term activities: increasing capabilities, competencies, provide intelligent, holistic security management, establish skills alignments(SFIA) decrease cybersecurity professionals shortage, because cybersecurity is our minds

1. Princples. 2. General and specific problems as a reason why such document shall be elaborated. 3. Current situation, good practices and problems. Institutional and societal awareness of cyber security problems

Governance framework for cybersecurity. Definition of missions, roles, tasks and responsibilities. Critical infrastructure protection.

CIIP

- Privacy - Critical Infrastructure - Open Internet - Cybercrime

Why the cybersecurity is relevant, how it helps to achieve the goals of society. Description of environment. Description of current state. Long term goals. Measurable goals for this concrete strategy. Dependencies and priorities between the goals. List of leading institutions who are responsible for different aspects of the strategy. Added should be implementation plan and required ressources.

1. CIP 2. management, responsibilities 3. incident detection/response

1) Cyber security „management", responsibilities, cooperation; 2) Cyber security awareness (various audiences ranging from the public to ICT industry to strategic-level decision makers in the government); 3) security of important national information infrastructure (vital services/critical infrastructure, government infrastructure etc.)

9. What is the best practice that can be transposed into the national cyber security strategy?(10 responses)

Good reporting systems for incidents and communication about solutions

Cooperation between public and private stakeholders

some of security standarts ISO, COBIT, NIST

Public and private partnership, build trust between public and private stakeholders. For instance, promotion of idea about responsible disclosure policy as a important tool against Zero day attacks.

A national strategy, if developed correctly, can meet many needs of government, the private sector and the citizens of the country. A strategy should be based upon six principles: • Risk-based. To develop a risk-based approach to managing national cybersecurity risks, countries must first create and articulate a framework for assessing national cyber risks and prioritizing appropriate protections. • Outcome

-focused. Focus on the desired end state rather than prescribing the means to achieve it, and measure progress towards that end state. • Prioritized. Adopt a graduated approach to criticality, recognizing that disruption or failure are not equal among critical assets or across critical sectors. • Practicable. Develop plans that are not overly prescriptive or burdensome so they'll be adopted by the broadest group of those in government and business. • Respectful of privacy and civil liberties. Include protections for privacy and civil liberties based upon privacy and civil liberties policies, practices and frameworks. • Globally relevant. Integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible.

trust and collaboration between stakeholders

Awareness and implementation guides

Did not understand the question.

step by step development from building awareness to capability building

Difficult to single out one example. There are many good practice examples in different strategies.

10. What is it that national cyber security strategies lack? What are the errors made in valid national cyber security strategies?(9 responses)

A good vision of the future. Most strategies only focus on parts of the national critical infrastructures (such as water, electricity and transport) but ignore others (such as healthcare institutions) and those latter sectors are insufficiently prepared to deal with system breakdown beyond the 96 hour emergency window.

irregular updates, upgrades, absence of adequate measures or S-M-A-R-T goals

In some strategies more attention have been paid for security of military facilities, objects, information systems, but much les, how to strengthen law enforcement capacities, how to support science in order to build new tools for public awareness. What sort of measures state shall envisage in order gather statistics concerning IT incidents, possible actions.

I would mention the lack of a proper set of goals and means to develop national capabilities and the necessary legal framework. I think modernizing the legal framework it is a must.

not applicable, this information should be acquired by the entities designing a strategy.

Pro-activeness because of lack of

Most common is lack of focus, everything is considered important. The other very common problem is considering cybersecurity as a technical problem. And there is also the lack of links to society, why other people tha cybersecurity specialists should care, no link to goals of society.

Adopting a strategy without allocating resources for implementing the decision.

Defining a NCSS document that is not rooted in national circumstances, i.e. nationally relevant cyber threat picture, organic organisational structure, realistic and available resources. Or a good strategy that is not implemented.

11. Which of the existing cyber security strategies do you see as the most advanced and why?(10 responses)

I'm not sure it is possible to point to one that is most advanced.

US, UK. If I'm not mistaken they should be amongst the first ones chronologically, and their capabilities in cyber ops are said to be top notch (which arguably partly depends from the funds allocated by the CSS)

The Cyber Security strategy of Norway are more internal oriented, highlighting importance of the business and the economy. There were good explanations about the processes of ICT security and the implementation of them into the private sector; the responsibility of the stakeholders and the consequences ignoring those guidelines.

Most comprehensive seems to me US strategy. This documents gives to stakeholders overall picture of current situation, measures to be done and how to build public awareness and strengthen law enforcement and judiciary.

The US strategy, the Netherlands and the UK - The US cyber security strategy unites electronic warfare and cybersecurity into a single concept called „full spectrum" so the objectives, scope and areas are different from other countries. - The Dutch cyber security strategy is one of the few who plan their responses based on international human rights agreements to justify the objectives of its plan. - The UK approach is concentrating on the national objectives linked to evolving cyber security: making the UK the major

economy of innovation, investment and quality in the field of ICT and by this to be able to fully exploit the potential and benefits of cyberspace.

not applicable (what does most adavanced mean? each strategy depicts the priorities of the country for a specific amount of time)

Critical infrastructure is evolving as fastest, so in my opinion it is the most advanced now. Most EU countries have (or will have very fast) legislation in place.

The best is „Strong Britain in the uncertain world" that defines the country defence strategy during cyber age. Their „Cyberstrategy" is not impressive. Also Netherlands have good strategy.

Netherlands: moving to capability building.

Czech Republic (focused, ambitious, yet realistic); Netherlands (realistic understanding of national strengths and risks, reflects overall national priorities); Estonia (focused objectives based on a realistic understanding of areas in need of improvement). For cyber security awareness, Austria 2013)

12. Should the national strategy contain a review of the current global and national cyber security situation on risks, emerging threats and vulnerabilities? Why?(10 responses)

Yes. Only by bringing the current and emerging risks/threats into a coherent picture is it possible to generate goals and strategies.

Yes. Real life scenarios are much more useful than ivory tower use cases.

yes, this is a mandatory control of security strategies in business environment, validate actual state of art

In very short and general way

It is a viable possibility; even though not necessary given that cybersecurity strategies often flow from the national security strategy.

yes

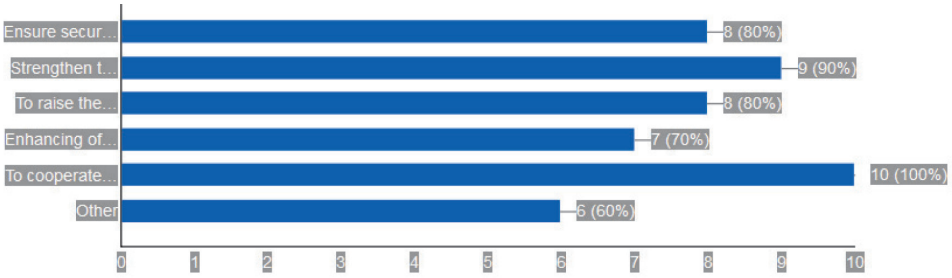
Since this is a continuous moving target, this (annual) review is essential for maintaining the effectiveness of the national cyber security policy..

It should refer to national defense strategy, where these definitions should be stated. Specifically it should state how those risks manifest themselves in cyber realm. The other basis document should be country economic and culture development plans.

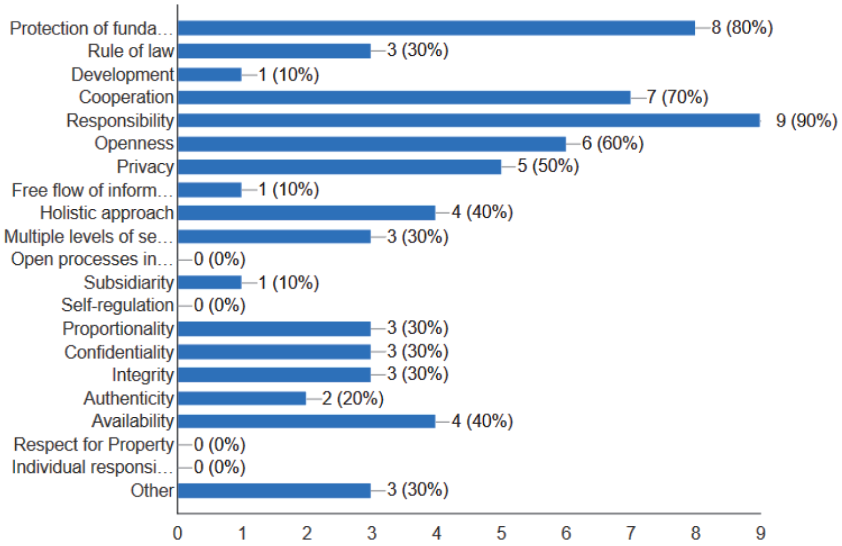
Yes, to identify the baseline for improvement and adopt to new or growing challenges/threats.

Yes rather than no, although the decision ultimately depends on national strategy culture and practice. The cyber security objectives and measures planned need to be (and also appear to be!) necessary, suitable, and proportionate. A review of the current threat picture, even if general, helps ensure that and also explain to the public why the measures intended are relevant. But the threat review can also be contained in a different document (e.g. periodic cyber threat assessment) and/or be generalised for the NCSS.

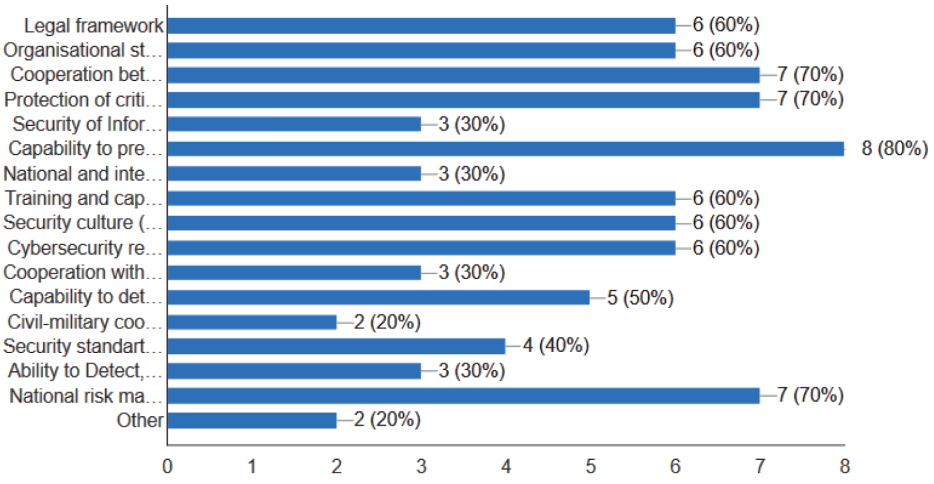
13. What strategic goals should be provided for in the strategy? Please select the most relevant goals in order of priority and enter other goals which you believe to be important:
(10 responses)



14. Do you think that principles should be provided for in the strategy? If „yes", please choose/ mention the principles which, in your opinion, must be indicated as mandatory:
(10 responses)



15. Do you think that the national cyber security strategy should provide for key areas of action? If „yes", please mark specifically:
(10 responses)



16. How internationality should be distinguished in the national cyber security strategy?(10 responses)

Include plans for cooperation with and learning from other countries; enhance communication between states

Cooperation mechanisms should be provided

cooperation agreements

One of the goals of strategy is to create guidelines for National stakeholders. In cooperation related with International stake holders, strategy may include separate chapter, where general principles of such cooperation has been developed.

- International cooperation: the effective protection against threats in cyber space unrestricted by geographical boundaries of countries or administrative boundaries of institutions is only possible through cooperation at both the national and international level, including the work of NATO, the EU, OSCE and UN, to promote the improvement of a secure, free and accessible cyber space. Support international efforts in enhancing mutual trust and cooperation, emphasizing the equal applicability of international legal norms to both the physical and the virtual environment. - Critical Infrastructure: Organize crisis training and security breach tests at a national, regional and international level. - Rule of law in cyber space and cyber crime: Facilitate discussions and exchange of opinions about the identification of new ICT crimes and improvement of the legal basis for the restriction thereof in line with the international trends. - Crisis situations: Develop regional and international cooperation, to ensure regular training for providing and receiving support in a crisis situation. - Awareness raising, education and research: Participate in international informative initiatives and platforms.

through collaboration

All cyberthreats are international, so it should (could) only be organized in an international framework to be effective.

Countries are dependent on their trade partners and allies.

If the certain country is NATO and/or EU member state it has responsibilities also in international cooperation, so it should be included.

Acknowledgement for the dependence of the country on international partners (e.g. for countering cyber crime, managing cyber-induced crises), need for international interaction and priorities in that regard (e.g. in international law and norms discussions).

17. Considering the international nature of cyber security and knowing that there are not many international regulatory acts unifying these issues, how could national cyber security strategies ensure efficient resolution of international issues (cooperation)?(9 responses)

Bilateral and multi-lateral agreements between states; public-private partnerships.

provide regular information flows

I don't know whether cyber security strategy should listed all possible cooperation forms and methods, I seriously doubtful about relevance.

- I think this question relies on bilateral and multilateral agreements at the highest political level, as well as on multinational end internationals organizations such as UN, NATO etc.

through international collaboration.

As I said above, it will only be of use when organized within an international framework (or multiple specialized frameworks - see 18)

Stratify the cooperation into layers. Leverage EU authority and power.

It is also the certain nation's need to support cooperation to build trusted environment to receive information/support. It should focus on the existing cooperation and the envisioned cooperation areas.

Identifying and aligning activities of allies and likeminded states.

18. How important is NATO and EU cooperation in the ensurance of cyber security? What are other countries, regions or organizations whose cooperation is of critical importance and real in pursuit of efficient cyber security ensurance? How detailed should the indication thereof be in the national cyber security strategy?(10 responses)

US and Canada are important cooperative partners. There should be indication of how other regions can use their intelligence resources and approaches.

a. I have no idea 2. I have no idea, the question is overly broad 3. high-level

important, Europol, European Cybercrime Centre, some description of functions and responsibilities

According to Information technology security law, CERT and MIL CERT has been authorized to carry out such cooperation concerning cyber security incidents. However in relation with cybercrimes, such obligation lays to special department of Ministry of interior. In my opinion in strategy, we should envisage only basic principles of such cooperation, but not details and special methods.

- NATO and EU cooperation it is vital since most of the global companies that operate and produce technology in cybersecurity sector belong to these countries. - NATO, EU, and UN are organizations which cooperation is of critical importance. - China, Russia, Japan and Korea are relevant countries wrt cybersecurity. - In my view the NCSS should mention that has been developed in line with documents of international organizations, especially the EU and NATO.

not applicable

EU is essential regarding international critical infrastructure and the legal framework. European Commission provides sevices on every element of the national cyber security framework. Nato only on cyberdefence, which is quite limited.

Look at your international trade, where are your critical supply chains and markets.

Very. If there are no action plans/acts covering the cooperation with international organisations it should be covered in the strategy. The organisations are depending on the interest of the country. OSCE, UN or other organisations can provide a platform for cooperation with nations not included in NATO or EU cooperation.

Both NATO and EU cooperation are important, but the organisations have different mandates and serve different purposes (also different audiences). For other international organisations, I'd refer to https://ccdcoe.org/incyder.html. The level of detail concerning international cooperation in NCSS is not very detailed normally, but should be phrased sufficiently clearly to identify national priorities and common interests for all institutions involved, considering that a country's „cyber interests" and realities are rather similar regardless of the different mandates of different organisations.

19. How and to what extent is cooperation of the public and private sector important in the cyber security area? How should it manifest? How should this be reflected in the strategy? Which private sector segments should be more involved in the cooperation?(10 responses)

The two sides really cannot work effectively without one another.

Fundamental; I have no idea of how the cooperation should manifest or be reflected in the strategy; tech manifacturers and communication providers, orgs running critical infrastructures, military/intelligence contractors, to name a few.

private sector engagement is very important and valuable, focused on business issues, don't forget critical infrastructure owners interests

definitely strategy should manifest principles for such cooperation and also give some good examples of such cooperation.

- Cooperation of the public and private sector is key for success. The need is for defining an appropriate mechanism (often a public private partnership) that allows all relevant public and private stakeholders to agree on different policy and regulatory cyber security issues. This should be stated in the NCSS by establishing and clarifying public and private sector roles. - The cyber security market does not only find its application in defense and aerospace, or government and public utility sectors, but are also critical for the IT domain, as well as other industrial, telecommunications equipment, manufacturing, Banking, Financial Services and Insurance (BFSI), healthcare, retail, and education sectors.

collaboration between public and private sector is very important and should be stated in the strategy. This can be done in many ways, through PPPs or working groups. One area of action that should include both the private and the public sector is the protection of critical information infrastructures and services.

Europol provides an essential international cooperation when targeting cybercrime.

Most of the critical infra is owned by and most of the specialists are employed by private sector. Goal is to protect society, not just state. Telcos, Banks, It companies, critical infrastructure, mass media, auditors.

Very. Most of the critical infrastructure is provided by them. It should provide a platform for open discussion and cooperation. The platform can be open and the relevant player can be invited.

The fact of private ownership of the majority of information infrastructure (communications networks) and private sector's role in developing cyber technologies and solutions already points to the area of potential cooperation. The natural cooperation partners are providers of vital services (including communications, energy, financial institutions heavily reliant on cyber).

20. Should an institutional cyber security model be provided for in the national cyber security strategy or other documents (such as laws)? Should functions and responsibilities be described?(10 responses)

Depends on which institutional level this question implies. But essentially, having a model is important for some private sectors that are only now waking up to these types of threats, as they can learn from established practices in the field.

Hardly, it'd arguably lead to a one-size-fits-all approach

yes

In very short and descriptive way. Of course it would be relevant that shortly function and responsibilities of main stakeholders, like Ministry of Defense, Ministry of Interior, Ministry of justice would be included.

- Yes indeed, consistent with the headings of the EUCSS. - Functions and responsibilities should be described.

The governance model should be clarified when implementing the strategy (it doesnt have to be described in the official document but the stakeholders involved should know their responsibilities in the implementation of the specific actions).

Yes, much exists already, the KU Leuven (University of Leuven - Legal department) did already a lot of work on it.

At least institutional blueprint and roles should be defined. Assignment to concrete institutions can be in implementation plan.

Yes, and it should be shared with partners to be able to identify the couterpart.

Strategy and law complement each other. The vision and objectives should be defined in NCSS, the specifics (esp. tasking) be addressed in legal acts.

21. Should the national cyber security strategy provide for measures to combat cybercrime? If so, what should they be?(10 responses)

I think this is more of a local level issue, but of course they are related and at overlapping points the strategy should indicate that.

No, too detailed, leave it to LEAs

Legal measures: Electronic signatures,Corporate responsibility, Definitions of important terms, Legal validity of electronic documents, Role of adjudicating officers, Requirements on data retention, Cybercrime reporting mechanism

yes. Firstly, strengten capacities of different stakeholders. Secondly - indicate necessary changes concerning Criminal, Criminal procedural legislation, Thirdly- ideas, proposals how to create awareness of society concerning given problem.

Yes indeed: - Legal Measures. - Appropriate national and regional organisational structures and policies on cybercrime - Global harmonisation is important because gaps in national legislation abet cybercrime. - The strategy may visualise and support the adoption of cybercrime conventions at the United Nations. - Legal measures should contain a governance structure to provide the Executive the legal mandate to mobilize all resources against cyber threats. - Relationships with global organisations such as the Interpol Cybercrime Unit and regional and national partners. - The cybersecurity strategy should addresses the need to improve judicial capacity against cybercrime. Strategists should build capacity to enable judges and prosecutors to gain a reasonable understanding of computers, software, networks and electronic evidence. In the short-term, countries may consider instituting training courses. In the long-term, it is important to modify curricula to ensure that lawyers and prosecutors obtain grounding in computer-enabled crime. The judiciary requires training in methods of handling electronic evidence to ensure that it preserves its evidential weight and thus admissibility in Court. - Typical participants include government departments, intelligence and law enforcement, private firms, civil society, academics and citizens.

adapt required legislation and ratify existing interantional treaties, create specialised national cyber crime units, continuous training, expertise and knowledge on cyber crime related threats and vulnerabilities, harmonised set of rules, foster cooperation between various players, involve public and private sectors

Yes, measures like, for example, securing private internet connections, to force banks to better secure their internet banking transactions,

Yes.

Yes

Substantive and procedural law issues, capacity of the law enforcement organisation in cyber crime prevention, investigation and prosecution. Training of personnel (law enforcement, prosecutors, judges).

22. Should the national cyber security strategy govern cyber defence issues? If so, how exactly should that be done?(10 responses)

Absolutely. No one solution, but cooperation between ministries is one important aspect, as is training for relevant agencies and actors.

Yes, from a high-level perspective, to be fine-tuned successively by the entities concerned/involved

regardless of size, degree of cyber risk or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience

Yes. I personally think that strategy shall be drafted in conformity with other similar documents, e.g. state security strategy, National State security law and others. It means that ideas and visions included into strategy should coincide , but not overlap mentioned documents.

- It is important to stress that when it comes to cyber security, research and development cannot be separated from defence-related activities. Scientific research is important primarily because the implementation of protective measures for information systems is a rapidly advancing high-technology field. Efficient protection against malware is possible only if new versions of the threat are immediately identified and neutralised. The priority areas for development include intelligent protection software and the simulation of cyber-attacks to ensure cyber security and provide training. - Some NCSS mention defence objectives by sharing their desire to become a world power in the area of cyber defence (France). - The strategy should aims at having improved cyber defence capabilities (Participation in EU cyber defence initiatives, capability building, technology development, identification and structure of military CERT, increased resilience through cooperation and new assets against military cyberattacks, faster detection, response and recovery from sophisticated attacks, cost efficient development through collaboration, robust, available and clear communication channels), in mid term to have improved resilience through cooperation and new assets against cyber attacks and in long term to have the level of cyber attack protection highly increased.

this should be examined per country depending on the priorities, there is no one size fits all solution

This is possible, hereby I think about the French way of working where Cyber security is close related to the Ministery of Defence.

Yes.

Do not understand the question.

At least to the extent necessary to deconflict with and peacetime activities of other (government) institutions and integrate the defence organisation's threat picture into national awareness and continuity management. Defence is not isolated from the state organisation, and especially not in cyber.

23. Should the strategy refer to issues of critical infrastructure? If so, please itemize them.(10 responses)

Better protection of all critical infrastructures, not just the big 3 (water, transport, electricity grids). Better capabilities for detection, response and reporting.

Yes, necessarily.

yes

Absolutely. Critical information infrastructure is essential for every country. In my view strategy shall include principles according to which system has been determined as part of such structure. Such information is also necessary, because it may assist possible stakeholders, whether their system has some probability to be enrolled into this list or not.

- Critical infrastructure protection (CIP) deserves special attention when discussing cyber security in general as well as government strategies. This is due to two factors. First, critical infrastructure concerns the protection of vital services for society to function and, as such, receives a higher priority and often more stringent security requirements due to their sensitive or delicate nature. Therefore, the mapping and identifying of services to be part of CIP is essential. The second factor concerns the lack of direct government control in the majority of Member States over the critical infrastructure sector, since most critical infrastructure are in the hands of private actors. - Cross-sectorial collaboration, information sharing within the industry and response mechanisms are elements to be dealt by the strategy.

yes it is number one priority. specific items: identification of CIIs, identification of operators of CIIs, risk assessement, minimum security measures per sector, incident reporting per sector, incident response per sector, enhance collaboration between private and public

Yes, energy and telecom are the most important, but also internet connected water, natural gas and transport.

Yes. First define what is critical.

Yes.

Cannot think of a reason to NOT consider critical infrastructure in a NCSS, especially given the heavy ICT-dependency of many critical sectors. Issues may include identification of information infrastructure components of vital services, increasing their resilience and reducing vulnerability, introducing a comprehensive cross-sectoral risk and security management, integrating cyber aspects of vital service continuity with national crisis response plans, managing vital cross-border dependencies on information infrastructure located outside of the country, etc.

24. Should the strategy describe standards, their application and marking for security purposes? If so, please itemize them.(10 responses)

Some technical standards that are critical to protecting infrastructures should be included, but again, this should be open enough to be flexible and deal with changes to the technology.

Too detailed, probably.

minimum requirements for different industries could be described in separate document

I don't think that strategy is a right document, which may create some security standards. It should be goal for specific legislative act.

- Not necessarily in the NCSS but in the corresponding plans.

no

Standards should only be applied within an international framework. For example, e-signatures on transactions etc.

Just state what standards there are and what is their role. Baseline security standards, specialist qualifications, sector specific service standards.

No. The strategy should cover what, who. The how can be in act or law.

National choice, but the issue of standards may be too specific for the strategic nature of a NCSS. Depends on how they are described as well.

25. Should the strategy implementation plan be a part of the national strategy, or should it be singled out into a separate document?(10 responses)

For clarity it would be better to be separate, but should be available in conjunction with the strategy as a „sister document".

What's a ‚national strategy'? I would see it as a standalone document.

could be different approaches, the result and change governance is most significant

Implementation plan should considered as an integral part of strategy

- At the national level the activities are often described and periodically updated through the implementation plans of the national strategies, which in turn are usually not published. The country's legislative framework provides for many of the activities (e.g. those involved in creating and revising new legislation). In some cases, such as the UK, where centralised funding is available, central government bodies are more heavily involved in defining the activities. However, in countries with more decentralised systems and where cyber security activities are financed out of the standing budget lines of the entities involved, such as the Netherlands, activities are sometimes designed by the departments themselves. - The NCSS should define the roadmap for the implementation of the strategy, which may involve the following steps. o Define concrete activities that would meet the objectives of the strategy. o Develop a governance framework for the implementation, evaluation and maintenance of the strategy. o Develop a master plan for the implementation of the strategy. o Develop concrete action plans for each activity. o Define the evaluation of the strategy and its main actions (e.g. which key performance indicators (KPIs)) will be performed and by whom.

depends on the priorities of the country, please read the ENISA good practice guides

I prefer to have special attention to this document, so to have is singled out. National politics usually discard everything cyber, and as a (small) part of national strategy it will never get the required attention.

Yes, it should be integrated into general plans but presented as separate document.

I would use separate for having easier update.

For the level of specificity that is necessary for realistic implementation, a separate document seems a better idea. But the decision ultimately also depends on national political culture and practice, the planned duration of the NCSS, the structure of the actual document, etc. The form should be decided based on the contents, not vice versa.

26. Could the implementation of the strategy be enshrined in respective laws and subordinate legislation?(10 responses)

yes
yes
Possibly, but there is a risk of piecemeal legislation leaving gaps - and that should be addressed by states.
I don't see why not; is it necessary, though?
When legislation have been submitted to the Parliament, Ministry or particular body attach also explanatory report or annotation which explains why such legislative act needs to be adopted. Generally it includes also references to strategy, planning documents, international guidelines etc.
- Yes, in order to be effective and to ensure that the different bodies can carry out their mandate and adhere to national and EU legislation
It should be!
Did not understand.
Yes.
This seems inevitable at least for measures that impact the rights and obligations of persons (e.g. industry and service providers, users). However, not all objectives can be reached by legislative means alone.

27. Which cyber security issues in the state should be left for self-regulation? How should the efficiency of self-regulation be increased?(9 responses)

No answer.
different requirements for small and medium-sized enterprises
Public private partnership and regulations for non- state bodies. State may intervene only in situation, if level of deficiency may reach such level that may jeopardy legal interests of persons.
One of the main challenges that is inherent to the use of self-regulatory initiatives is that membership, as well as adherence of their members to agree upon rules is entirely voluntary. Especially in the area of cyber security information sharing, this can pose a problem, as companies and governmental actors are hesitant to share information about their vulnerabilities, given that such sharing can lead to reputational loss especially when the information becomes public. A major deterrent to the voluntary sharing of information is a lack of trust between participants in any given sector, especially in a cross-border context. To address this challenge, face-to-face meetings to build trust and encourage sharing amongst participants is necessary. Another challenge of self-regulation compared to traditional regulation is the lack of mechanisms to enforce agreed upon rules. This can be overcome by warning and excluding members in case of non-compliance to the set rules. In any case it is worthy to analyse the roles and responsibilities of existing public agencies mandated to deal with cyber security policies, regulations and operations (i.e energy regulators, electronic communications' regulators, data protection authorities, national cyber crime centres); identify overlaps and gaps. And to assess the extent to which the existing policy, regulatory and operational environment meet the objectives and scope of the strategy; If not, identify the missing elements.
depends on the priorities of the country
Very little, self regulation is not working when it comes to safety and security since it is not the primary interest of the subjects. It only (can) apply when it is in the interest of the subjects, like busines efficiency.

Market analysis should be done and regulated should be just public goods, where the whole ecosystem benefits. All other things should be left for self regulation.

The self regulation and efficiency can be incised through, providing consultations and sharing best practices in the community.

First, leaving an issue for self-regulation need not mean leaving this issue out of the NCSS - the government may still want to articulate a desired outcome in an area, even if the choice of measures does not include regulation. Not everything contained in a NCSS should automatically be regulated. Awareness-raising, information exchange, research and development will likely benefit more from a non-regulatory approach (such as incentive programmes, cooperation from government). For example, substantial and meaningful cooperation in information sharing, especially between private and public sectors, tends to be more effective in a non-mandated setting where both parties gain value out of the relationship.

Priedas Nr. 3. Lietuvos ekspertų aprašymas

Vytautas Butrimas (Lietuvos Respublika) – Lietuvos Respublikos krašto apsaugos ministerijos, Kibernetinio saugumo ir informacinių technologijų departamento vyr. patarėjas, Lietuvos Respublikos ryšių reguliavimo tarnybos Tarybos narys.

Dr. Algirdas Kunčinas (Lietuvos Respublika) – Valstybinės duomenų apsaugos inspekcijos direktorius.

Renata Mačiulevičienė (Lietuvos Respublika) – Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos Saugos skyriaus vedėja.

Dr. Rytis Rainys (Lietuvos Respublika) – Lietuvos Respublikos ryšių reguliavimo tarnybos Tinklų ir informacijos saugumo departamento direktorius.

Vitalij Dmitrijev (Lietuvos Respublika) – Lietuvos Respublikos Seimo Nacionalinio saugumo ir gynybos komiteto Biuro vadovas.

Arvydas Plėštys (Lietuvos Respublika) – Lietuvos Respublikos krašto apsaugos ministerijos, Kibernetinio saugumo ir informacinių technologijų departamento direktorius.

Marius Pareščius (Lietuvos Respublika) – International security cluster vadovas, UAB „Infosistema“ vadovas, Užupis creative cluster vadovas.

Saulius Japertas (Lietuvos Respublika) – Kauno technologijos universiteto Telekomunikacijų katedros vedėjas.

Priedas Nr. 4. Klausimai Lietuvos ekspertams ir Lietuvos ekspertų apibendrinti atsakymai

Ekspertų atsakymai:

1. Kokie struktūros elementai ir / ar turinio aspektai turėtų būti akcentuojami kaip svarbiausi Lietuvos nacionalinėje kibernetinio saugumo strategijoje? Gal galite išskirti, jūsų nuomone, aktualiausius / būtiniausius elementus / aspektus?

Penki ekspertai paminėjo, kad būtina akcentuoti kritinės infrastruktūros apsaugą. Vienas iš šių penkių ekspertų pavystė toliau mintis dėl kritinės infrastruktūros. Jis nurodė, kad visų pirma reikia identifikuoti objektus, kuriuos reikia saugoti. Antra, reikia identifikuoti kokios institucijos turi užtikrinti kritinės infrastruktūros apsaugą. Ir trečia, būtina identifikuoti, kokios institucijos yra atsakingos už kibernetinių pažeidimų padarinių koordinavimą. Du ekspertai paminėjo institucinę struktūrą/sistemą kaip itin svarbų strategijos elementą.Vienas iš šių dviejų ekspertų paminėjo, kad svarbu, kad būtų apibrėžtos konkrečios institucijų funkcijos. Du ekspertai nurodė, kad strategijoje svarbu išskirti tikslą, t.y. tai, ko siekiama strategija. Vienas ekspertas nurodė keletą strategijos elementų: valstybės informacinius išteklius, kibernetinius nusikaltimus, organizacinius- techninius gynybos gebėjimus, kibernetinės kultūros vystymą, teisinę bazę ir tarptautinį bendradarbiavimą. Kitas ekspertas nurodė tokius galimus strategijos elementus: tikslus, principus, objektus. Vienas ekspertas nurodė, kad strategijoje svarbu išanalizuoti esamos būklės situaciją bei nurodyti darbus ir uždavinius.

2. Kokiose probleminėse srityse ypatingai turėtų pasireikšti Lietuvos nacionalinis kibernetinio saugumo strategijos kontekstas?

Vienas ekspertas rizikingiausiu sektoriumi nurodė atominės energetikos objektus. Pagrindiniais konkrečiais problematiškiausiais sektoriais (3 ekspertai iš 8) įvardino energetiką ir finansus, tačiau išskiriami ir specifiniai, pvz.: transportas, telekomunikacijos, sveikatos apsauga, chemijos ir maisto pramonė, karinė infrastruktūra, dujų sektorius, paslaugos gyventojams (registrai, duomenys).

3. Kokie principai turėtų būti KSS?

Du ekspertai, kalbėdami apie strategijos principus, paminėjo strategijos ir LR Kibernetinio saugumo įstatymo santykį. Jie nurodė, kad strategija turėtų remtis principais, kurie yra nurodyti Kibernetinio saugumo įstatyme; vienas iš šių ekspertų dar pridūrė, kad principų lygmenyje svarbu apibrėžti privatumo ir saugumo santykį. Kalbėdami apie bendruosius arba specialiuosius principus, du ekspertai nurodė, kad strategijoje turi būti ir bendrieji, ir specifiniai kibernetinio saugumo principai; vienas iš šių dviejų ekspertų nurodė, kad tiek bendrieji, tiek specifiniai kibernetinio saugumo principai turi būti suderinti. Vieno eksperto nuomone, strategijoje turi būti nurodyti bendri principai, neišskiriant specialiųjų (pavyzdžiui techninių) principų. Kiti ekspertai apklausos metu nurodė skirtingus principus, kurie turėtų būti numatyti strategijoje. Vienas ekspertas paminėjo, kad turi būti išankstinio perspėjimo ir aktyvios gynybos principas, kitas ekspertas nurodė, kad turi būti prevencijos principas, trečias ekspertas nurodė orientavimosi į rezultatą principą, ketvirtas ekspertas išskyrė bendradarbiavimo tarp verslo, akademinio pasaulio ir valstybės, tinkle neutralumo, anonimiškumo, neutralumo principas.

4. Kaip formuluotumėte Lietuvos KS strategijos strateginį tikslą (-us)?

Ekspertų įžvalgos apie strategijos strateginį tikslą (-us) yra skirtingos. Vieni ekspertai išskiria tik vieną tikslą. Vienas ekspertas įvardijo, kad strategijos tikslas yra užtikrinti kritinės informacinės infrastruktūros nepertaukiamą funkcionavimą ir kuo greitesnį galimų pasekmių likvidavimą. Kitas ekspertas ekspertas nurodo, kad strategijos tikslas yra gerinti būseną, prisidėti prie gerinimo, numatyti etapus ir galimas priemones. Kiti ekspertai išskiria daugiau tikslų (iš trijų dedamųjų). Vienas iš šių ekspertų nurodo, kad strategijoje turėtų būti vienas tikslas su 3 dedamosiomis: 1.užtikrinti saugumą, 2. užtikrinti laisvos raiškos galimybę, 3. užtikrinti socialinius-ekonominius privalumus. Kitas ekspertas taip pat nuorodo strategijos tikslą kaip galimą atsakymą į tris pagrindinius klausimus:1. nustatyti saugotinų objektų sąrašą, 2. nustatyti, nuo ko objektus reikia saugoti, 3. Nustatyti, kaip saugoti tuos objektus. Dar vienas ekspertas nurodo, kad strategijoje turi būti tikslas formuluojamas per sekančius klausimus: kokias atakas turi atlaikyti, kiek laiko atlaikyti ir per kiek laiko turi būti reaguojama į kiekvieną incidentą. Kiti ekspertai išskiria strategijos tikslą iš dviejų sudedamųjų dalių. Vienas ekspertas nurodo, kad strategijoje gali būti įtvirtintas vienas iš tikslų: 1. apsaugoti infrastruktūrą, 2. apsaugoti valstybės teikiamas paslaugas piliečiams, jo nuomone, strategijoje turėtų būti 1 ar 2 tikslai, kurių detalizuoti nereikėtų. Kitas ekspertas nurodo, kad strategijoje gali būti keli tikslai, vienas iš jų: harmoningas kibernetinio saugumo užtikrinimas šalyje su elektroninių ryšių plėtra ir technologijų vystymu. Paskutinysis ekspertas nurodo, kad strategijos tiksle turi atsispindėti šie klausimai: minimalus internetas visuose namuose, aprašyti kokybiniai parametrai, interneto priežiūra, turinys turi būti prieinamas ir saugus. Taip pat šis ekspertas, kalbėdamas apie strategijos tikslą išskyrė edukacijos svarbą.

5. Kokie turėtų būti Lietuvos „key areas of action“?

Ekspertų nuomonės apie strategijos Lietuvos „key areas of action“ yra skirtingos. Tik du ekspertai nurodo po vieną „key areas of action“. Vienas iš jų nurodė, kad Lietuvos „key areas of action“ turi būti valstybinių institucijų, dirbančių su kibernetiniu saugumu kompetencija. Kitas iš šių dviejų ekspertų nurodė, kad kad Lietuvos „key areas of action“ turi būti siejamas su lėšomis, kad kiekviena institucija galėtų planuoti lėšas savo saugumui ir toks planavimas turėtų būti valstybės lygiu. Daugelis ekspertų išskiria keletą Lietuvos „key areas of action“. Vienas ekspertas nurodė, kad Lietuvos „key areas of action“ yra susiję su 3 pagrindiniais klausimais: 1. nustatyti saugotinų objektų sąrašą, 2. nustatyti, nuo ko objektus reikia saugoti, 3. nustatyti, kaip saugoti tuos objektus. Kitas ekspertas išvardijo tokius Lietuvos „key areas of action“: kritinės informacinės infrastruktūros identifikavimą; atsakingų struktūrų už kibersaugos užtikrinimą bei jų hierarchizacijos identifikavimą; galimų grėsmių kėlėjų identifikavimą; reagavimo į kritinės informacinės infrastruktūros pažeidimą ar grėsmes plano sudarymą; pasekmių į galimus pažeidimus likvidavimo koordinatoriaus identifikavimą. Trečias ekspertas išvardijo tokius Lietuvos „key areas of action“: valstybės informaciniai ištekliai, kibernetiniai nusikaltimai, organizaciniai-techniniai gynybos gebėjimai, kibernetinės kultūros vystymas, teisinė bazė ir tarptautinis bendradarbiavimas. Ketvirtas ekspertas išvardijo tokius Lietuvos „key areas of action“: švietimas (šis ekspertas akcentavo vartotojų žinojimą bei supratimą apie kibernetinio saugumo problematiką), prevencija, kibernetinė gynyba. Penktasis ekspertas išvardijo tokius Lietuvos „key areas of action“: kritinės infrastruktūros apsauga, valstybinio sektoriaus apsauga ir švietimas. Dar vienas ekspertas išvardijo tokius Lietuvos „key areas of action“: tinklai ir elektroniniai ryšiai, finansai, energetika, kriminalistika, švietimas.

6. Kokia geriausia kitų valstybių praktika, kurią galima būtų perkelti į Lietuvos nacionalinę kibernetinio saugumo strategiją?

Keletas ekspertų išskyrė tas pačias valstybes, kurių geriausią praktiką galima būtų panaudoti kuriant Lietuvos kibernetinio saugumo strategijos modelį. Keturi eksperai paminėjo Estijos, kaip turinčios labai pažangią kibernetinio saugumo strategiją, pavyzdį. Trys ekspertai paminėjo JAV kaip valstybės, turinčios ilgametę patirtį. Du ekspertai paminėjo Vokietijos gerąją praktiką. Du ekspertai paminėjo Latviją, kaip valstybę, turinčią Lietuvai tinkantį kibernetinės strategijos modelį. Kiti du ekspertai paminėjo Izraelį, kaip praktinių sprendimų kibernetinio saugumo srityje pasiekusią valstybę. Kiti du ekspertai nurodė Olandiją kaip pažangią ir pagal teritprijos dydį atitinkančią Lietuvos modeliui strategiją. Vienas ekspertas pateikė praktinį kibernetinės atakos identifikavimo pavyzdį Izraelyje: buvo uždarytas tunelis, kadangi operatoriai staiga prarado vaizdo stebėjimo sistemas, priešgaisrines ir oro ventiliacijos sistemas. CERT negalėjo padėti, tačiau padėjo pusiau privati kompanija CyberJim, jie darė pratybas su pramoninėmis sistemomis ir jie nustatė, kad tai buvo kibernetinė ataka. Vienas ekspertas išskyrė Jungtinės Karalystės kibernetinio saugumo strategijos modelį, kuriame verslas ir jo geriausi darbuotojai yra įtraukiami Į CERT. Dar vienas ekspertas išskyrė Lenkijos strategiją kaip galimą geriausios praktikos pavyzdį, kuriame yra svarstomi kritinės infrastruktūros klausimai. Dar vienas ekspertas paminėjo Norvegiją kaip valsybę, turinčią atskirą CERT pramoninei infrastruktūrai.

7. Kokie tarptautiškumo elementai turėtų būti išskiriami Lietuvos nacionalinėje kibernetinio saugumo strategijoje?

Keletas ekspertų išskyrė panašius tarptautiškumo elementus Lietuvos kibernetinio saugumo strategijoje Trys ekspertai išskyrė pagrindinį reikiamą elementą strategijoje – bendradarbiavimą. Du ekspertai apibūdino bendradarbiavimo svarbą ES ir NATO kontekste (vienas ekspertas paminėjo konsultacijas su atitinkamomis ES ir NATO struktūromis (ekspertais)), bendradarbiavimą su kaimynais, du ekspertai išskyrė bendradarbiavimą su Latvija ir Estija, vienas iš iš šių ekspertų išskyrė taip pat Rusiją ir Baltarusiją. Vienas ekspertas, kalbėdamas apie tarptautiškumo elementus išskyrė Lietuvos aktyvų dalyvavimą NATO kompetencijų centre Estijoje. Taip pat dar vienas ekspertas išskyrė ES vieningos strategijos ir bendrų principų svarbą. Vienas ekspertas išskyrė tokius tarptautiškumo elementus, kaip dalinimąsi informacija, pasitikėjimu grindžiamos visuomenės ir kolektyvinių priemonių sukūrimą. Vienas ekspertas akcentavo, kad reikėtų tarptautiniu lygmeniu turėti Jungtinių tautų įstaigą, kuri prižiūrėtų įgyvendinimą, atliktų monitoringą. Dar vienas ekspertas paminėjo, kad svarbu nustatyti tarptautinio bendradarbiavimo prioritetus, kaip pavyzdžiui, CERT, ENISA (praktinė, operatyvinė) ITU, interneto valdymo forumas. ReIkėtų pasirinkti sritis, kur turėtų būti taikomas tarptautinis bendradarbiavimas.

8. Kokie viešo ir privataus sektoriaus bendradarbiavimo aspektai turėtų būti įtraukti į Lietuvos kibernetinio saugumo strategiją?

Atsakydami apie viešo ir privataus sektoriaus bendradarbiavimo aspektus du ekspertai nurodė, kad kibernetinio saugumo srityje viešo ir privataus sektoriaus bendradarbiavimas yra labai žemo lygio ir turi būti vystomas. Strategijoje viešo ir privataus sektoriaus bendradarbiavimas turėtų būti grindžiamas geranoriš-

kumu, kontaktu, kasdieniniu bendravimu. Reikia rasti tinkamas bendradarbiavimo formas, nes šiuo metu yra nemažai spragų, pvz. susijusių su viešaisiais pirkimais. Trys ekspertai paminėjo apsikeitimo informacija svarbą. Vienas iš šių ekspertų nurodė į ryšio pasiekiamumo didinimą, visiems dalyviams, tiek viešo, tiek privataus sektoriaus turėtų būti vienodas ryšio pasiekiamumas ir turėtų vykti bendri projektai kibernetinio saugumo srityje. Kitas ekspertas nurodė į privataus ir viešo sektorių partnerystės kibernetinio saugumo srityje vystymą. Trečias ekspertas šalia viešo ir privataus sektorių dar nurodė ir akademinės bendruomenės įtraukimą. Vienas ekspertas paminėjo ekspertinių konsultacijų svarbą dėl viešo ir privataus sektoriaus bendradarbiavimo aspektų. Jo manymu, tikslingiau būtų kalbėtis su nepriklausomais ekspertais iš mokslo ir studijų įstaigų. Kito eksperto nuomone, didelio skirtumo tarp privataus ir viešo neturėtų būti. Į strategiją turėtų būti įtraukiama tik aspektų, kiek yra reikalinga visuomenei. Dar vieno eksperto nuomone į strategiją turi būti įtraukti visi sektoriai, pramonė ir pan., kas dalinai priklauso ir privačiam sektoriui.

9. Keleriems metams turėtų būti priimta Lietuvos nacionalinė kibernetinio saugumo strategija?

Kalbėdami apie Lietuvos nacionalinės kibernetinio saugumo strategijos galiojimo laikotarpį, ekspertai turėjo skirtingas nuomones, atkreipdami dėmesį į keletą svarbių su strategijos galiojimo laikotarpiu susijusių aspektų. Tokie aspektai yra susiję su kibernetinio saugumo srities dinamika ir ypač greitu vystymusi. Apibendrinant ekspertų atsakymus galima sugrupuoti į dvi skirtingas grupes: 1. Ekspertai, pasisakantys už ilgalaikę strategiją ir 2. ekspertai, pasisakantys už trumpesnio laikotarpio strategiją. Keturi ekspertai nurodė, kad strategija turėtų būti ilgalaikė. Viena iš šių ekspertų apibrėžė, kad strategija turi būti „ilgalaikė“, kitas ekspertas nurodė konkretų terminą – 10 m., kitas nurodė, kad turi būti ilgalaikė 10 m. strategija, ketvirtas ekspertas nurodė, kad strategija turi būti nuo 5 m. iki 10 m. Pagrindiniais ilgalaikės strategijos argumentais ekspertai įvardijo itin greitą ir dinamišką technologijų, geopolitinės padėties, o taip pat ir grėsmių kitimą. Vienas iš šių ekspertų paminėjo, kad ši ilgalaikė 10 m. strategija turėtų būti peržiūrima kas 3 m. Trys ekspertai pasisakė už trumpesnio laikotarpio strategiją. Vienas iš šių ekspertų paminėjo, kad reikia po poros metų išleisti naują strategijos versiją. Reikia nuolat vertinti, ar kibernetinio saugumo klausimai pasikeitė, reikia iš naujo įvertinti pagrindines strategijos dedamąsias dalis. Du ekspertai nurodė, kad kibernetinio saugumo srityje labai greitai viskas kinta, todėl turi būti pastoviai atnaujinama. Vieno iš šių eksperto nuomone, daugiau nei 5 metams strategijos neįmanoma parengti. Bendri principai išlieka (jų galima nekeisti taip dažnai), bet kita dalis gali būti atnaujinama (peržiūrima) kas metai, pvz. dėl grėsmių. Kitas ekspertas tiesiog paminėjo, kad 4–5 m. būtų racionalus terminas kibernetinio saugumo strategijai.

10. Ar Lietuvos nacionalinėje kibernetinio saugumo strategijoje turėtų būti numatytas institucinis kibernetinio saugumo modelis? Ar reikia aprašyti funkcijas ir atsakomybes?

Dėl institucinio kibernetinio saugumo modelio ekspertų nuomonės buvo skirtingos. Du ekspertai be jokių papildomų komentarų atsakė, kad turi būti numatytas institucinis kibernetinio saugumo modelis. Keturi ekspertai laikėsi nuomonės, kad strategijoje nereikėtų detalizuoti atsakomybių, kibernetinio saugumo įstatyme visos atsakomybės konkrečiai įvardintos. Vienas iš šių ekspertų pridūrė, kad reikia aprašyti reikiamas valstybės funkcijas. Kitas iš šių ekspertų pridūrė, kad strategijoje turi būti tikslai, uždaviniai, siekiamybė. Trečias iš šių ekspertų nurodė, kad reikia vystyti, kokios jau dabar yra institucinės funkcijos, ir naujų nekurti. Visi kiti ekspertai turėjo nuomones su papildomais komentarais dėl kibernetinio saugumo institu-

cijų. Vieno eksperto nuomone, kai kuriais atvejais institucinis kibernetinio saugumo modelis būtų sunkiai įgyvendinamas. Kiekviena kritinės infrastruktūros šaka yra savotiškai unikali. Ir bendru atveju būtų sunku rasti viena instituciją, kuri galėtų užtikrinti visų šakų realią apsaugą. Šio eksperto manymu, tikslinga būtų turėti instituciją su funkcijomis ir atsakomybe, kuri koordinuotų bendrą politiką šioje srityje bei instituciją, kuri organizuotų pasekmių likvidavimą. Kito eksperto nuomone, turi būti pagrindinė institucija, susijusi daugiau su civiliais. Krašto apsaugos ministerijai nelabai tinka kibernetinio saugumo klausimus kuruoti, nes vienintelė priemonė – karas. Gal net daugiau Ūkio ministerijai reikėtų pavesti. Kitas ekspertas nurodė, kad vidaus reikalų ministerija galėtų būti koordinuojančia ir atsakinga institucija už kibernetinį saugumą.

11. Ką reikėtų įtraukti į Lietuvos kibernetinio saugumo strategiją, kad jos nuostatos nebūtų tik deklaratyvios?

Vieno eksperto nuomone, strategija ir yra deklaratyvus dokumentas. Po jos yra parengiamas veiklos planas, kuris ir padės išvengti vien tik deklaratyvumo. Kitas ekspertas panašiai nurodė, kad strategija – susivokimo dokumentas, todėl į ją svarbu įtraukti apie dabartinę situaciją, grėsmes, apsaugos priemones, galbūt priemonių planą. Vienas ekspertas paminėjo priemonių plano įtraukimą, kad būtų išvengta deklaratyvumo. Kito eksperto nuomone, tinkamas lėšų skyrimas valstybei padės išvengti deklaratyvumo. Dar vienas ekspertas akcentavo kontrolės institucijos sukūrimu (angl. – Chief Information Officer), kuris kuris rūpinasi informaciniais resursais ir kibernetine sauga. Vienas ekspertas siūlė išskirti prioritetus, kad būtų nesistengiama apimti visko, o imti konkrečius prioritetus. Dar du ekspertai, atsakydami į šį klausimą labiau orientavosi į pačios strategijos turinio klausimus. Vienas iš jų paminėjo, kad turi būti išsprendžiami trys dedamieji strategijos klausimai, kitas nurodė, kad būtina akcentuoti tam tikrų institucijų vadovybės atsakomybę, įtraukti į strategijos ruošimą tokių žmonių, kurie yra ne analitikai (o jų paprastai institucijose nėra), kurie mato problematiką plačiau ir globaliau.

12. Ko reikėtų vengti kuriant nacionalinę kibernetinio saugumo strategiją?

Keturi ekspertai išskyrė, kad reikėtų vengti abstraktumo, neapibrėžtumo. Vienas iš jų akcentavo, kad reikėtų vengti per daug atsargių formuluočių, konkrečiai nustatyti saugotinų objektų sąrašą, nustatyti nuo ko objektus reikia saugoti, 3. Nustatyti, kaip saugoti tuos objektus. Be to, reikėtų bijoti deklaruoti asmeninę (ar bent jau institucinę) atsakomybę ir nekalbėti apie finansus. Kitas iš šių ekspertų paminėjo, kad Lietuvai reikalingas konkretesnis atvejis ir konkretesnės nuostatos. O vėliau galima pereiti prie deklaratyvesnio varianto. Šiai dienai Lietuva dar nėra subrendusi deklaratyvioms nuostatoms. Kitas iš šių eskpertų įvardijo, kad reikėtų vengti aprašomojo pobūdžio, geriau rinktis praktinį pobūdį, orientuotą į konkrečius rezultatus, konstatuojamųjų normų – minimaliai. Paskutinysis iš šių ekspertų detalizavo, kad reikėtų prisirišimo prie konkrečių technologijų, taip pat vengti vienpusio valstybės dalyvavimo kibernetinio saugumo įgyvendinime. Valstybė turi naudotis verslo resursais. Kiti keturi ekspertai turėjo atskiras nuomones dėl to, ko reikėtų vengti. Vienas iš jų nurodė, kad reikėtų vengti rožinio požiūrio, kad bus greitai pasiekiami rezultatai. Kitas ekspertas paminėjo, kad reikia vengti, kad strategiją rašytų uždara grupė. Reikia viešų konsultacijų. Turi būti visi įtraukti į rengimą. Trečias iš šių ekspertų nurodė, kad reikėtų vengti tokių tekstų, kaip buvusi 2011 m. VRM patvirtinta programa su daugelių priemonių, tikintis, kad jos bus įgyvendintos. Be to, nenusismulkinti į detales, o rengti bendresnio pobūdžio dokumentą. Nebandyti visko

išspręsti, o apimti sritis, kurias strategija būtų pajėgi išspręsti. Paskutinis iš šių ekspertų nurodė, kad reikėtų vengti pavadinimų, valstybių, organizacijų, technologinių sprendimų aprašymo.

13. Kaip įsivaizduojate siektiną/idealų kibernetinio saugumo modelį?

Trys ekspertai pasisakė, kad idealaus strategijos modelio nėra. Vienas iš šių ekspertų pridūrė, kad strategija – procesas, todėl idealumo čia nėra. Kitas iš šių ekspertų pajuokaudamas išsakė nuomonę, kad galbūt išjungti internetą, nes visiško saugumo nėra, turi būti balansas tarp žmogaus teisių ir saugumo. Paskutinysis iš šių ekspertų nurodė, kad Lietuvai reikėtų laikytis Europinės strategijos linijos bei neišradinėti dviračio iš kiekvienos šalies paimant po tinkantį perliuką. Turi būti konkreti, maža, siaura, trumpesniam laikotarpiui, pragmatiška, nes 4–5 m greitai praeis ir po jos sieks tobulesnė strategija. Kiti ekspertai turėjo skirtingas nuomones dėl idealaus / siektino Lietuvos strategijos modelio. Du ekspertai pasisakė, kad jei būtų įgyvendintos strategijos turinio dedamosios dalys, tai ir būtų siektinas kibernetinio saugumo modelis. Vienas ekspertas ypač išskyrė švietimo svarbą, jis susiejo idealios strategijos modelį su vartotojų ir institucijų branda. Šis ekspertas pabrėžė, kad švietimas prasideda jau nuo mokyklos laikų. Jau būnant mokykloje reikia išmanyti pagrindinius kibernetinio saugumo principus, apie programų atnaujinimus, valdyti interneto šaltinius. Kitas ekspertas įvardijo, kad siektinas modelis turi būti kintantis, kadangi grėsmės dinamiškos. Turi būti įtvirtinamas persitvarkantis ir įvertinantis naujausius dalykus modelis. Paskutinysis ekspertas paminėjo, kad gali būti keletas siektinų modelių: 1 Įprastas, 2. Sustiprinto režimo (kai kažkas trukdo) bei suformuoti pajėgumai lygiagrečiai su institucijomis.

Autorių pastabos:

Keli ekspertai negalėjo išvardinti konkrečių problematiškų sektorių, kuriuose turėtų ypatingai pasireikšti Lietuvos nacionalinis kibernetinio saugumo strategijos konktekstas. Principai labai skirtingi, keli rekomenduoja sieti su Kibernetinio saugumo įstatymu.

Kalbėdami apie viešo ir privataus sektorių bendradarbiavimą, ekspertai nurodė, kad tai jautriausias, subtilus klausimas. Sunku subendrinti ekspertų atsakymus. Ekspertų mintys labai skirtingos. Net jeigu kažkurios mintys sutampa, dalis tų minčių prasmės skiriasi. Ekspertai vertina viską pragmatiškai, be iliuzijų. Strategijos modelis turi būti konkretus, aiškus ir tikslus be ypatingo deklaratyvumo.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2016 Volume 4 Number 2 (December)

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/

PRECONDITIONS OF SUSTAINABLE ECOSYSTEM: CYBER SECURITY POLICY AND STRATEGIES[1]

Darius Štitilis [1], Paulis Pakutinskas [2], Inga Malinauskaitė [3]

[1,2,3] Mykolas Romeris University, Ateities str.20, Vilnius, Lithuania

E-mails: [1] stitilis@mruni.eu; [2] paulius.pakutinskas@mruni.eu; [3] inga.malinauskaite@mruni.eu

Received 17 May 2016; accepted 25 August 2016

Abstract. Ten years have already passed since the first cyber security strategies were drawn up in different countries reflecting global cyber security policy. The aim of this scientific article is to analyze the historical development of cyber security strategies of selected EU and NATO countries and to reveal future trends of cyber security policy. The article examines key elements of the selected strategies in the initial cyber security strategies and the description thereof in the already improved cyber security strategies. We selected countries with different allegiances. First, we chose two countries that are members of both the EU and NATO (the Netherlands and Estonia), then a country, which is only a member of NATO, namely, the United Stated of America, thirdly, an EU state, which is not a member of NATO, namely, Finland. We believe the research results may be used for both the development of current cyber security strategies, as well as well as for drafting a cyber security policy.
Keywords: cyber security strategy, historical development, entrepreneurship, policy

Reference to this paper should be made as follows: Štitilis, D.; Pakutinskas, P.; Malinauskaitė, I. 2016. Preconditions of sustainable ecosystem: cyber security policy and strategies, *Entrepreneurship and Sustainability Issues* 4(2): 174-182.
DOI: http://dx.doi.org/10.9770/jesi.2016.4.2(5)

JEL Classifications: O33; D80

1. Introduction

More and more countries have become some kind of victims of cyber-attacks on the one hand, and have realized the seriousness of cyber-attacks and the importance of cybersecurity on the other hand (Ventre D., 2015; Allabouche, et al. 2016; Samašonok, et al. 2016; Belás, et al. 2016). The concept 'cyber security' emerged in the1990s, when the increasing dependence of the public on the development of information technologies was observed. Cyber security is associated with the creation and maintenance of processes related to the identification of emerging cyber threats and costs for the application of reasonable countermeasures (Shoemaker and Conklin, 2012). Cybersecurity is not an isolated objective, but rather a system of safeguards and responsibilities to ensure

[1] *This article is part of the research 'Analysis and adaptation of EU and NATO cyber security strategies: Lithuanian cyber security model', funded by the Research Council of Lithuania (Grant No. MIP-099/2015/PRC-36).*

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2016 Volume 4 Number 2 (December)

the functioning of open and modern societies (Klimburg A., 2012), also it`s a precondition of sustainable ecosystem. The United States Computer Science and Telecommunications Board, which conducts scientific research in the field of cyber security each year, noted that cyber security is the main challenge of public policy (2015). Key components of cyber security are laid down in the main strategic documents, namely, cyber security strategies. In other words, cyber security strategies define and institutionalize the national cyber security system (Cezar, 2013).

The aim of this article is to reveal future insights into and tendencies of cyber security strategies. Origins of the cyber security regulatory initiatives may be associated with fragmented legal provisions in certain sectors. However, with the increase in cybercrime, the need to have new regulatory initiatives creating presumptions for a unified cyber security regulation has been growing. Documents in the cyber security area first appeared in the early 2000s. Russia adopted the National Security Concept of the Russian Federation in 2000; in 2003, the US passed the National Strategy to Secure Cyberspace; in 2005, Germany adopted a National plan for Information Infrastructure protection. It should be noted that for the most part these first documents were not yet referred to as cyber security strategies; they were more like plans, security strategies, information security strategies or strategies on critical infrastructures on the basis whereof countries later adopted cyber security strategies.

There has been a remarkable increase in the adoption of cyber security strategies since 2011. This was when most EU member states and other countries adopted cyber security strategies. For example, Luxembourg adopted its cyber security strategy in 2011, Georgia – in 2012, Italy – in 2013, and Denmark and Iceland – in 2014. Regional Cyber Security Strategy of the European Union approved in 2013 and Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union adopted in 2016. The objective of this Directive is to achieve a high common level of security of network and information systems in the Union while adopting minimum harmonisation requirements. It is noteworthy, that several countries have already adopted second versions of their cyber security strategies. The goal of this article is to research the historical development of the cyber security strategies of the selected European Union and NATO countries.

2. Methodology

Countries, whose cyber security strategies have demonstrated a significant change have been selected for the research. The research has been carried out by analyzing the content of the initial and second cyber security strategies of the selected countries. In particular we assessed constituent elements of cyber security strategies, such as threats and challenges, principles, methods, key goals and implementation. These particular elements were chosen because it was noted they were key composite elements of both initial and second strategies, and comprehensively disclose the content of cyber security strategies. The course of the research evaluates the change of constituent elements of strategies throughout their history, examines how the content of the selected cyber security strategies has changed over time, solves issues and proposes methods to address various questions.

Countries that are members of the European Union and NATO, as well as those that are members of NATO or the European Union alone, were chosen for the research analysis. First, countries belonging to both the European Union and NATO, namely, the Netherlands and Estonia were chosen. Then, for further comparison of the historical development of cyber security strategies, a country which is a member of NATO alone, namely, the USA, was selected. And finally an EU member state which is not a member of NATO, namely, Finland. These four countries have already adopted second cyber security strategies. This different level of participation by countries in international organizations is believed to be able to reveal trends of cyber security strategies, and also to reveal regional cyber security perspectives.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2016 Volume 4 Number 2 (December)

3. National Cyber Security Strategies of the Netherlands of 2011 and 2013

The Netherlands adopted its first cyber security strategy in 2011. The first part of the strategy contained the presentation of the issue, principles and goals of the cyber security policy. The second part of the strategy established specific actions, which the Government had to implement together with other cooperating authorities. The first strategy of the Netherlands formulated fundamental cyber security principles, such as promotion of public and private partnership, active international cooperation, allocation of responsibilities between ministries, etc. The aim of the strategy was security and confidence in an open and free digital society. The second part of the strategy enshrined a specific action plan, including but not limited to the establishment of a cyber security council and the national cyber security centre, assessment of threats and risks, enhancement of the protection of critical infrastructures, development of possibilities to repel potential attacks, investigation of cybercrime and promotion of research and education.

The second cyber security strategy of the Netherlands was adopted in 2013. It emphasized the correlation between security, freedom and socioeconomic benefits. One of the fundamental principles enshrined therein is that responsibilities applicable in physical space should also apply in cyber space. Thus, in order for a dialogue on cyber security between various stakeholder groups to reach a new level of maturity, three key elements should be considered: the development of self-regulation, transparency and awareness. The second strategy clearly allocates the responsibilities of different authorities, namely, it identifies areas of responsibility of the government, the business sector and individuals.

The historical development of the cyber security strategies of the Netherlands can obviously be characterized by a significant change in its constituent elements. This valuable change of elements is reflected in a comparative table of key constituent elements of the cyber security strategies:

Table 1. Comparison of strategies

National Cyber Security Strategy of the Netherlands of 2011	**National Cyber Security Strategy of the Netherlands of 2013**
Partnership between public and private sectors	Participation of private and public sectors
Focus on structures	Focus on networks/strategic coalitions
Formation of a model of various related authorities	Refinement of responsibilities of related authorities
Capacity-building in the Netherlands	Capacity-building both in the Netherlands and other countries
General approach: distribution of capacities for enhanced protection measures	Risk-based approach: balance between protection of interests, threats and acceptable risks in society
Formation of fundamental principles	Presentation of policy (vision)
From ignorance to awareness	From awareness to capability

Table 1 specifically illustrates the changing approach to specific cyber security strategy elements. A change from the formation of initial elements to the refinement of specifics is seen. For example, where the first strategy

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2016 Volume 4 Number 2 (December)

formulated fundamental principles of cyber security, the second strategy establishes the presentation of policy (vision). Where the initial strategy formulated the model of related authorities, the second ones focuses on more specific responsibilities. The internationalization method of the cybersecurity phenomena should be noted. The second strategy of 2013 emphasizes capacity building both in the Netherlands and abroad and focuses more on the capabilities with the overall assumption that awareness has already been reached. The second strategy of the Netherlands also highlights a specific action plan laid out in the Annex to the strategy according to each goal.

4. National Cyber Security Strategies of Estonia of 2008 and 2014

The achievements which Estonia made in the area of cyber security came to light in 2007 when Estonia was the first country in the world to be the target of cyber-attacks. Shortly afterwards, in 2008, Estonia adopted its first cyber security strategy. The strategy has a very clear structure – an introduction, cyberspace threats, actions in the cyber security area, enhancement of cyber security in Estonia and implementation of cyber security. According to the Estonian Cyber Security Strategy of 2008, national implementation of cyber security should be based on such principles as cooperation between public and private sectors, protection of critical infrastructure, awareness raising etc. Cyber security threats are defined in the Estonian Cyber Security Strategy of 2008 as potential attacks, which are carried out remotely, using minimal resources and resulting in severe consequences. The action plan emphasizes the protection of Estonian information society and information infrastructure, security of information systems, practical trainings in the area of information security as well as the importance of legal cyber security regulation and international cooperation. To describe legal regulation in the Estonian strategy, a comprehensive review of key documents of international, regional and national legislation as well as of aspects of cooperation of international organizations was conducted.

In 2014, Estonia adopted a new cyber security strategy. It should be mentioned that the Estonian Cyber Security Strategy of 2008 was also considered to be one of the most advanced strategies in Europe (Laasme, 2012). Thus, the new strategy has consistently continued the implementation of most of the goals set in the strategy of 2008. Moreover, the new strategy incorporates new threats and needs, which were not provided for in the previous strategy. It should also be noted that when it comes to content, the new Estonian strategy is more concise. The strategy of 2014 analyses the current situation (the progress achieved in separate sectors, cyber security trends and other challenges). The increasing dependence of Estonia as a country, as well as of its economy and residents on information technology and electronic services is identified as the main challenge. The need for modern legal regulation has been highlighted as additional activity to repel threats listed in the new strategy. When comparing the principles laid down in the Estonian strategy of 2008 and the strategy of 2014, most of the principles identified in the strategy of 2008 can be seen to have prevailed in the strategy of 2014, with the only difference being in the formulation thereof. The main goal provided for in the Estonian Cyber Security Strategy of 2014 for the next four years (2014–2017) is to increase cyber security capabilities and raise the population's awareness of cyber threats, while at the same time ensuring continued confidence in cyber space. The last part of the Estonian strategy of 2014 describes the related authorities responsible for strategic actions and lays down specific deadlines for the implementation of the actions.

In summarising the comparison of both strategies we notice some profound insights. First, a very important aspect of cyber security phenomena – continuity. The new strategy has consistently continued the implementation of most of the goals set in the strategy of 2008. Second, one outcome of this continuity is that many aspects in the second strategy remain the same, only the formulation differs slightly. The second strategy is found to be more concise, itemizing principles of cyber security, the overall objective of the strategy and additional goals.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2016 Volume 4 Number 2 (December)

5. National Strategy to Secure Cyber Space of the United States of 2003 and US International Strategy for Cyber Space of 2011

The first cyber security strategy document of the United States appeared in 2003 when the National Strategy to Secure Cyberspace was adopted. Compared to the strategies of the Netherlands and Estonia examined above, this strategy can be distinguished for its comprehensiveness and scope. In terms of content, the strategy consists of an introduction, threats and vulnerabilities of the cyber space, the national policy and tendentious principles as well as five priorities of the national cyber security.

The National Strategy to Secure Cyberspace of the US of 2003 emphasizes the efforts and priorities of the organization. It also establishes the direction for the actions of government and other organizations. Moreover, this document identifies specific actions to be undertaken by state and local governments, private companies and organizations as well as individuals in order to achieve a higher level of cyber security. Unlike the European cyber security strategies (the Netherlands and Estonia), the US has included each US citizen since 2003, emphasizing that everyone can contribute to the creation and development of cyber security. It is notable, that even if the strategy of 2003 is comprehensive, it distinguishes only three strategic goals. The 2003 National Strategy to Secure Cyberspace presents a vision stating that the protection of cyber security is a complex and constantly evolving challenge. The strategy mentions that this document is the first step to protecting information infrastructures in the long-term. The strategy mentions and distinguishes functions and responsibilities of federal and local governments.

The US International Strategy for Cyberspace was adopted in 2011. Its content consists of four parts: 1. Building cyberspace policy. 2. Cyberspace's future. 3. Policy priorities. 4. Moving forward. Cyber security regulation requires a coherent policy and media attention; it is a complex regulation of state and federal government, including various regulatory methods and areas of application (Thaw, 2014). Thus, the US strategy of 2011 emphasizes a strategic method based on success building, principles and recognizing challenges. This strategy is based on fundamental principles, such as respect for fundamental freedoms, recognition of privacy and free movement of information. The goal of the US International Cyberspace Strategy of 2011is to work at the international level in order to promote open, interconnected, secure and reliable information and communication infrastructure, which supports international trade and commerce, strengthens international security and fosters free expression and innovation. The appropriate response to cybercrime can be achieved solely through international cooperation (Rosenzweig, 2012). In order to achieve this goal, the USA has been constantly building an environment with existing norms of responsible actions, reliable partnership and the support of the country's cyberspace under the rule of law. It should be noted that the development of such cyberspace norms in the country means that the country's actions have become predictable, and misunderstandings leading to conflict situations can be avoided. The idea behind the development of cyberspace norms emphasized in the strategy can also be found in scientific doctrine examining the occurrence of potential proactive cyber security norms in international law (Craig, Shackelford, Hiller, 2015).

Unlike other cyber security strategies, the US strategy of 2011 emphasizes the contribution of the United States themselves into the future of the strategy. The diplomatic goal of the United States is to develop initiatives and a common understanding of the international environment, where the states would work together as related responsible authorities. Moreover, the strategy mentions that the states should strengthen partnership, protection, security of information networks and deterrence against hostile acts.

Summing up it might be concluded that compared to the European strategies, both US strategies emphasize the involvement and contribution of each individual to the cyber security improvement process. Another difference of the US strategies might be noticed in the description of the aims of the strategies. While both strategies are very

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2016 Volume 4 Number 2 (December)

comprehensive, both establish three (2003 strategy) and only one (2011 strategy) goal. In addition, the aspect of cyber security as a global matter is stressed in both of the US strategies.

6. National Information Security Strategy of Finland of 2008 and Cyber Security Strategy of Finland of 2013

The National Information Security Strategy adopted in Finland in 2008 is aimed at making each day in the information society secure and reliable for everyone. The vision of the strategy is the confidence of these bodies in the fact that information is secure when using various communication technologies and related services. The priorities of the National Information Security Strategy of Finland of 2008 establish the principles for the protection of a critical information society and international network cooperation. Finland is an integral part of the global information economy, and many threats are of international nature. Therefore, resistance to such threats is based on good preparation and efficient expansion of the international cooperation network and a clear vision of the future in the identification of threat signals.
The Cyber Security Strategy of Finland was adopted in 2013. The content of the strategy consists of four parts and annexes [24]: 1. Introduction. 2. Vision for cyber security. 3. Cyber security management and the national approach. 4. Strategic guidelines for cyber security. The strategy presents the vision, approach and strategic guidelines of cyber security. Unlike other strategies, this one establishes that cyber security is not exclusively a legal category, the adoption whereof would mean the conferral of new competences to institutions and other state establishments. Thus, this strategy is not aimed at creating new responsibilities and powers for the authorities.

The vision of Finland's cyber security is that Finland can secure its vital functions against cyber threats in all situations. Citizens, authorities and businesses can effectively utilize a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally. Finland's strategy of 2013 is linked to the national information security strategy of 2008. It establishes that cyber security depends on efficient organization of information security. In other words, cyber security regulation is viewed holistically. Thus the implementation of cyber security is based on efficient and all-inclusive collection of information and the analysis thereof nationally and internationally. This is the only way in which comprehensive preparedness against cyber-attacks can be achieved. Good management of cyber security allocates responsibilities and functions among state authorities, private entities and the public. Cyber security must meet functional and technical requirements. The strategy mentions investments and trainings in research and development and the fact that Finland will contribute to these initiatives. By way of conclusion it might be stated that similar to the Estonian case, Finland emphasizes the element of continuity in drafting the strategy of 2013.The trend of moving from the level of fundamental provisions to a more strategic approach can be noticed in the comparison of both documents. However, unlike other countries, the new strategy of 2013 establishes that cyber security is not exclusively a legal category, thus this strategy is not aimed at creating new responsibilities and powers for the authorities.

Conclusions

The historical development analysis of cyber security strategies of all the countries above revealed one essential feature – the change of document provisions, which undoubtedly reflects the progress of cyber security in real life. The strategies obviously have to reflect the real life situation (Rosenzweig, 2012). From our analysis of the different cyber security strategies, we have noticed several important trends.

At first, if the initial strategies talked about the formation of fundamental provisions, the second ones had a more specific focus, such as the presentation of policy and vision. The first strategies emphasized structures and the formation of a model of responsible authorities, while the second strategies focus on strategies and refinement of

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2016 Volume 4 Number 2 (December)

institutional responsibilities. The first strategies raised awareness of cyber security, while second strategies talk about the development of abilities in the cyber security area. The second strategies are more specific and most of them enclose specific action plans in the cyber security field.

The second, the analysis also revealed the importance of the global approach in cyber security phenomena. The majority of first strategies emphasized the cyber security capacity-building inside the country itself, while almost all the second strategies emphasize the building of capacities internationally. A particularly significant example of the current tendency is revealed in the analysis of the US strategy of 2011. While emphasizing the internationality of cyber security, the diplomatic goal of the US is to create initiatives and a common understanding of the international environment, which would work for the mutual benefit of cyber security. In so doing, the US assumes liability for cyber security of the entire international community.

The third, the consistency approach in building future cyber security strategies can be noted. Many second cyber security strategies emphasized the criterion of continuity. For example, since the Cyber Security Strategy of Estonia of 2008 was an advanced document, the second Cyber Security Strategy of 2014 distinguishes the emphasis on continuously developing confidence in cyber space. The US cyber security strategy of 2011 stresses the predictability of cyber security, which might be linked with the consistency approach.

The fourth, the planned specific deadlines for the implementation of the strategies can be distinguished herein as one of the progress indicators contained in the provisions of many second generation strategies themselves. Planned specific deadlines emphasize specific matters, certain actions and authorities responsible. Planned deadlines refer to the achievement of the results.

Acknowledgements

This article is part of the research 'Analysis and adaptation of EU and NATO cyber security strategies: Lithuanian cyber security model', funded by the Research Council of Lithuania (Grant No. MIP-099/2015/PRC-36).

References

Allabouche, K.; Diouri, O.; Gaga, A.; El Amrani El Idrissi, N. 2016. *Mobile phones' social impacts on sustainable human development: case studies, Morocco and Italy*. Entrepreneurship and Sustainability Issues Vol. 4. No. 1, pp. 64-73. DOI: http://dx.doi.org/10.9770/jesi.2016.4.1(6)

Bambauer D. E., 'Schrodinger's Cybersecurity'. University of California: *Davis Law review*. Vol. 48. No. 3. 2015. p. 798.

Belás, J.; Korauš, M.; Kombo, F.; Korauš, A. 2016. *Electronic banking security and customer satisfaction and in commercial banks*. Journal of Security and Sustainability Issues Vol. 5 No.3, pp. 411-422. DOI: http://dx.doi.org/10.9770/jssi.2016.5.3(9)

Cezar P., Cyber security – current topic of national security. *Public security studies*. Vol. II. No. 4(8). Dec 2013. p. 25

Craig A.N., Shackelford S.J, Hiller J. S., 'Proactive cybersecurity: a comparative industry and regulatory analysis'. *American business journal*. March 2015. [interactive] [2015] [viewed on 23-11- 2015] SSRN: http://ssrn.com/abstract=2573787

Cyber security strategies of all countries of the world and years of adoption thereof are available on the website of ENISA. [interactive] [2015] [viewed on 2015-11-09]. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2016 Volume 4 Number 2 (December)

Cyber Security Strategy of the European Union [interactive] [2015] [viewed on 26-10-2015]. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Cyber Security Strategy of the Netherlands of 2014. p.8. [interactive] [2015] [viewed on 18-11-2015]. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union. [interactive] [2016] [viewed on 19-09-2016]

Estonian Cyber Security Strategy of 2014. p.7. [interactive] [2015] [viewed on 23-11-2015]. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies ncsss/Estonia_Cyber_security_Strategy.pdf

Estonian Cybersecurity Strategy of 2008. p. 7. [interactive] [2015] [viewed on 18-11-2015. http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Klimburg A. *National Cybersecurity Framework Manual*. NATO CCDCOE, 2012. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

Laasme H.. The role of Estonia in developing NATO'S cyber strategy. Cicero foundation great debate paper. No.12/18. 2012. P. 9. [interactive] [2015] [viewed on 23-11- 2015] SSRN:http://www.cicerofoundation.org/lectures/Laasme_%20Estonia_NATO_Cyber_%20Strategy.pdf

National Cyber Security Strategy of Finland of 2013. [interactive] [2015] [viewed on 29-12-2015]. https://ccdcoe.org/cyber-security-strategy-documents.html.

National Cyber security Strategy of the Netherlands of 2011. p.3. [interactive] [2015] [viewed on 18-11-2015]. https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

National Strategy to Secure Cyber Space of the United States of 2003 [interactive] [2015] [viewed on 29-12-2015]. https://ccdcoe.org/cyber-security-strategy-documents.html .

Rosenzweig P., 'Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?' *A journal of law and policy for the information society*. Vol. 8(2). 2012. p. 398.

Sales N.A., 'Regulating Cybersecurity'. *North-western University Law Review*. Vol. 107. No. 4. p. 1567.

Samašonok, K.; Išoraitė, M.; Leškienė-Hussey, B. 2016. *The internet entrepreneurship: opportunities and problems*, Entrepreneurship and Sustainability Issues Vol. 3 No. 4, pp. 329-349. DOI: http://dx.doi.org/10.9770/jesi.2016.3.4(3)

Shoemaker, D.; Conklin, A., *Cyber security: the Essential body of knowledge*. Course technology. 2012. p. 11.

Thaw D. The efficacy of cybersecurity regulation. *Georgia state university law review*. Vol. 30(2). 2014. p. 291

The United States Computer Science and Telecommunications Board research, accessed online. [interactive] [2015] [viewed on 05-11-2015] http://sites.nationalacademies.org/CSTB/index.htm

Ventre D., *Chinese Cybersecurity and Defense*. London, John Wiley & Sons, Inc, 2014.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2016 Volume 4 Number 2 (December)

Darius Štitilis is professor at the Mykolas Romeris University. He obtained PhD degree in law from Mykolas Romeris university in 2002 (the topic of Phd Thesis was related to the legal responsibility in cyberspace). He is the executive manager of master study program "Cyber cesurity management" at Mykolas Romeris University. His research interests include IT law, cyber security law, privacy and personal data protection law, electronic identification law, cybercrime. He has over 40 publications primarily in the field of law and IT. Under his direction, he was involved in several scientific EU and national projects. Also, he is the co-author of two scientific monographs regarding identity theft in cyberspace: legal and electronic business issues, and e-health.
ORCID ID: orcid.org/0000-0002-9598-0712.

Paulius Pakutinskas is associated professor at the Mykolas Romeris University. He obtained PhD degree in law from Mykolas Romeris university in 2009 (the topic of Phd Thesis was related to the legal regulation of electronic communications). His research interests include IT law, intellectual property, cyber security. Also, he is the co-author of scientific monographs regarding identity theft in cyberspace: legal and electronic business issues.

Inga Malinauskaitė is a lecturer and PhD student at the Mykolas Romeris University. Her PhD topic is related to regulation and protection of data subject's rights in online social networks. Her research interests include data subject's rights, data protection in relation to IT systems, intellectual property, cyber security, online security issues.
ORCID ID: orcid.org/0000-0001-5693-7300

MYKOLO ROMERIO UNIVERSITETAS

University of Salford A Greater Manchester University
University of Essex ESSEX BUSINESS SCHOOL International Centre for Entrepreneurship Research
The General Jonas Žemaitis Military Academy of Lithuania
Ministry of National Defence Republic of Lithuania
Vilnius Gediminas Technical University
RISEBA
Estonian Business School
NATO Energy Security Centre of Excellence
ENTREPRENEURSHIP AND SUSTAINABILITY CENTER
AVADA

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2016 December Volume 6 Number 2
http://dx.doi.org/10.9770/jssi.2016.6.2(1)

CONCEPTS AND PRINCIPLES OF CYBER SECURITY STRATEGIES

Darius Štitilis[1], Paulius Pakutinskas[2], Uldis Kinis[3], Inga Malinauskaitė[4]

[1,2,4]Mykolas Romeris University, Ateities st. 20, LT-08303 Vilnius, Lithuania
[3]Rigas Stradins university, Latvia

E-mails: [1]stitilis@mruni.eu; [2]paulius.pakutinskas@mruni.eu; [3]uldis.kinis@gmail.com; [4] inga.malinauskaite@mruni.eu

Received 17 March 2016; accepted 26

Abstract. In the last few decades, the understanding of security has been changing. New areas emerged which may influence security facets, which were not urgent earlier. Now those facets can endanger individual persons or even states. Breaches of cyber security, separate attacks or intense cyber wars are becoming more usual than conventional wars in the physical space; violations of cyber security may cause great damage, ruin businesses or even temporarily paralyze full-fledged functioning of individual states or regions. Many countries of the world, realizing that such a threat is real, adopted Cyber Security Strategies; for some countries, this is not the first version of such a strategy. This article examines the place of Cyber Security Strategies in the system of state documents, the nature and importance of such strategies as well as whether they are binding on individuals and institutions. The article explores in more detail the principles of ensuring cyber security provided for in such strategies, i.e. the principles identified by the states, as important for ensuring cyber security. It is discussed why these principles are so different in the strategies of individual states.

Keywords: concepts, principles, cyber security, European Union (EU), North Atlantic Treaty Organization (NATO).

Reference to this paper should be made as follows: Štitilis, D.; Pakutinskas, P.; Kinis, U.; Malinauskaitė, I. 2016**.** Concepts and principles of cyber security strategies, *Journal of Security and Sustainability Issues* 6(2): 197–210. http://dx.doi.org/10.9770/jssi.2016.6.2(1)

JEL Classifications: F5, F52, K42, K24

1. Introduction

Increasing possibilities of hardware and software, growing Internet speed and importance of wired and wireless data transfer, the emergence of big data and cloud computing services, take-over by smart phones of increasingly more human communication functions, and emerging of other functions important to people means that information technologies play an increasingly more important role in our lives (Fuschi, Tvaronavičienė 2014; Laužikas et al. 2015; Ignatavičius et al. 2015; Grubicka, Matuska 2015; Rezk et al. 2015; Tvaronavičienė et al. 2016; Allabouche et al. 2016; Pauceanu 2016; Rezk et al. 2016; Samašonok et al. 2016; Prause 2016; Korauš et al. 2016). Information technologies are common not only in personal relationships, business, but also in state governance, military systems (which, historically, had a strong impact on the development of this area), science, etc. There are few areas where information technologies do not have an important or decisive impact. Such penetration of information technologies influences many areas of life, and this influence is so major that disturbances to information systems may paralyze one or another function of the state. For this reason, possible occupation or disturbance of information systems, or another impact thereon, are of interest not only to individual offenders or organized mafia groups, but also to official states and their governments, however, often they do not make such activities public or even deny and hide them. Dependence of human activities on information technologies will only increase in the future. Technological achievements are developing in a very

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online

dynamic manner, this also influences possibilities to have an adverse impact, using such technologies, on many areas of human activities, both those mentioned above and those not mentioned, therefore, the issues related to cyber security become increasingly more important. It is easiest for the states to fight adverse phenomena on their territories and jurisdictions, while cyberspace virtually defies state borders, therefore, development of cyber security on an inter-regional and international level becomes an important factor. This study will examine why the present strategies are still so different and whether a possibility exists to single out common principles so that all states find it easier to seek cyber security objectives.

In order to assess the formal preparedness of states to address cyber security questions, it is necessary to analyze regulatory acts and other documents issued by them. In many states, an important constituent part of documents is Cyber Security Strategies. To be able to evaluate the place of these documents in the system of documents of states as well as the importance thereof, it is necessary to answer several particularly important questions, which will be analyzed in this article. It is also crucial asses the means, used for regulation of social relations in the area of cyber security and the typical principles (of a certain field of social sciences) which are used or new principles, which are created exclusively for addressing cyber security issues.

Novelty and originality. In the drawing-up of cyber security strategies and other regulatory acts, it is vital to elaborate on the principles for the creation and development of a cyber security strategy as well as the development and further implementation (application) of legal norms. So far, a more thorough piece of research of cyber strategies has not yet conducted. It is reflected by practice, because the majority of strategies identify different principles and a different content thereof.

A practical and scientific significance. Having identified the place of a strategy - as a document, in the system of documents, as well as the purpose thereof and having systematized and elaborated on the principles of cyber security strategies, it will be easier to develop and improve cyber security strategies and other regulatory acts.

The purpose. To single out and systematize the principles of cyber security strategies.

Methods: Analysis of cyber security strategies and other regulatory acts as well as of scientific literature, comparative analysis, the systematic method.

2. Emergence of Cyber Security Strategies

The first cyber security strategies started to emerge as from the year 2000, however, only 2011 saw a real boom of Cyber Security Strategies and the majority of member states of the European Union and part of the states of the world approved their strategies[1]. That was a period of a break-through when states not only started to consider cyber security issues, but also finally identified them in documents as one of the most important security threats of one's country. Alas, it has to be noted that in democratic states, at least a few years of democratic discussions and coordination of the document elapse, until the approval of a specific document (in this case, a Cyber Security Strategy), i.e. at least one to two years pass as from the realization of cyber security threats, as a fundamental security threat, until the approval of the strategy. During this period, many areas of state activity became dependent on computers, the Internet and other elements of the electronic space. These data is reflected in various types of statistics, for instance, on e-government prevalence, e-banking development, etc. One of the simple and illustrative pieces of data illustrating the turning-point in the importance of cyber security is the number of households with Internet access and the number of individuals using the Internet. We can compare the correlation between the dates of emergence of the strategies and the prevalence of the Internet, which is presented in the charts provided below (Fig. 1, Fig. 2).

[1] More information is available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online

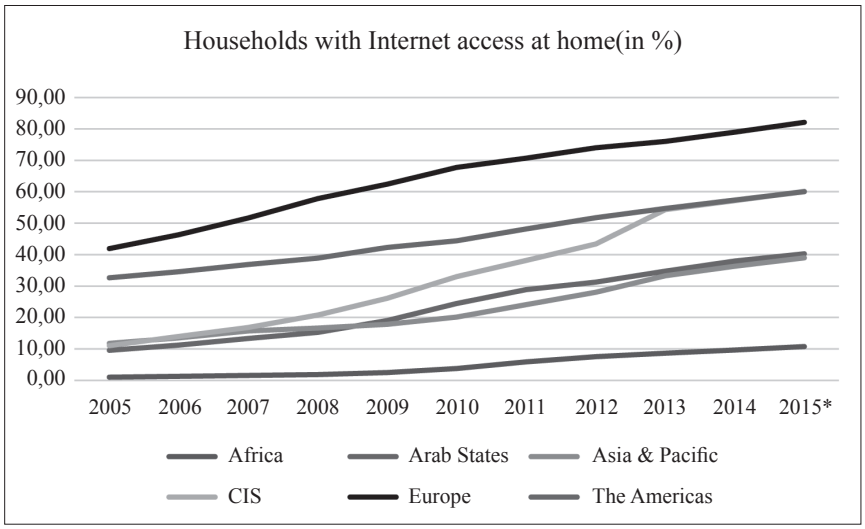


Fig.1. Internet access at home

Source: ITU World Telecommunication/ICT Indicators database.

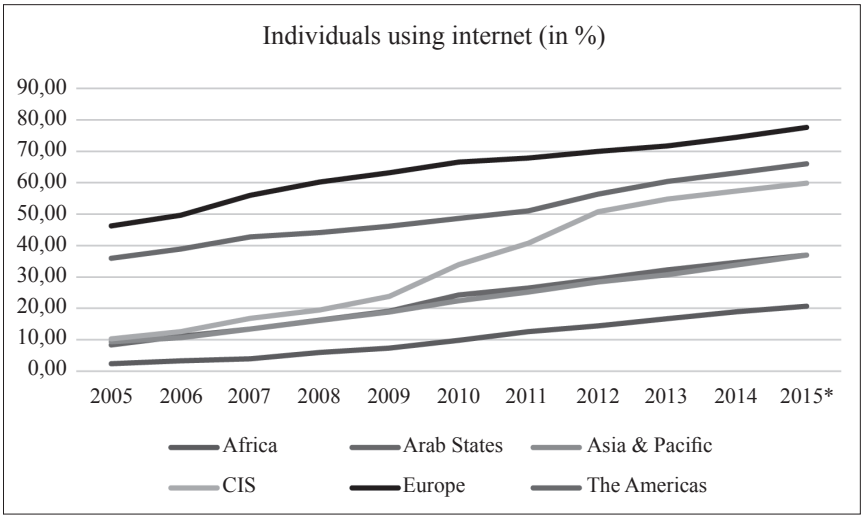


Fig.2. Internet users

Source: ITU World Telecommunication/ICT Indicators database.

It is noteworthy that since the time when, in the leading markets (Europe and America), about 40 per cent and more of users and households started using the Internet, the issue of cyber security has become critical.

It is also important to take into account the prevalence of breaches of cyber security. Every year, target groups and organizations of cyber attacks are different, however, the presented charts show what a wide circle of interests is violated by cyber attacks. It should be noted that the interests of a state are violated not only by those attacks which are aimed directly at the government, but also by the ones which are also able to have an adverse effect on other critical infrastructures and organizations or otherwise disturb the activities of a state or members of society (Fig. 3).

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online

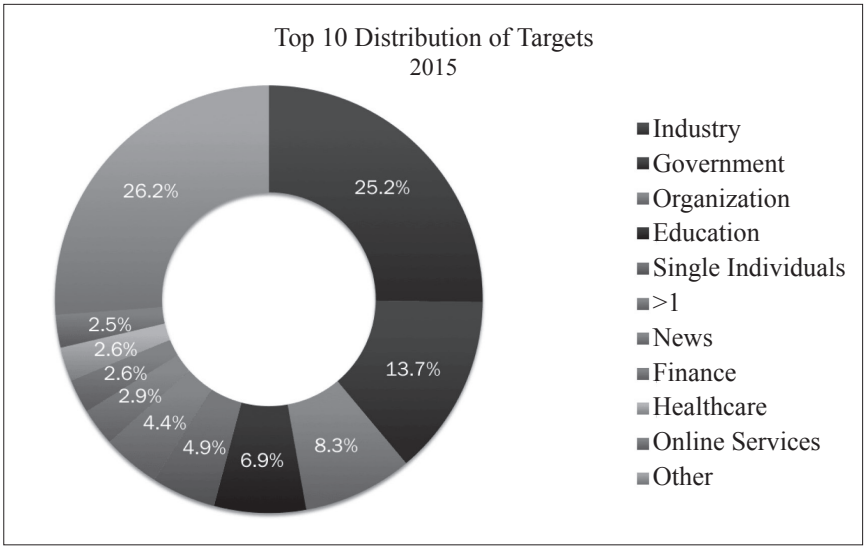


Fig.3. Targets, Organizations and attack statistic

Source: http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/

3. Why are Strategies Important?

Once we have identified that cyberspace is, or rather violations of relations created in this space are, a security threat, we face questions, which has to be addressed, and these questions differ from the questions and solutions thereto known to us historically. We will not find cyber security answers either in classical management, or in the military science or law, even though such problems as security, wars, crimes or legal regulation are not new and have a long history. What, then, makes this entire question so specific? Convergence of all these questions, following a change in technological possibilities, makes cyberspace and threats arising therefrom a qualitatively new question requiring a new approach and solutions.

The compilation of all questions, mentioned above in this chapter, and the knowledge possessed into one place does not give a uniform result; it is also confirmed by the variety of effective strategies, even though there are initiatives to make them more uniform (e.g. the EU's and other initiatives), however, so far even cyber security strategies of neighbouring countries or countries with a similar pattern of development have been particularly different. Overall, the objective of all cyber security strategies is similar, because of the intention to fight insecurity challenges in cyberspace and regulate them, however, the description of achieving these objectives and the realization thereof as well as the very strategy documents are very different.

4. Security, Definitions and Changes in the Understanding of the Problem

When talking about cyber security we are addressing fundamental security questions, which were understood in a completely different manner at the beginning and in the middle of the previous century. Especially after the Second World War, security has found major attention in the fields of International Relations and its subdiscipline, security studies. Security studies evolved during the nuclear age and were originally foremost about the study of the threat, use and control of military force, as one proponent of security studies, Stephen Walt, stated. They were mainly concerned with the military strategy and giving policy advice to the military[2]. Since the cold war, the study of security has come a long way. Most importantly, as Emma Rothschild has reminded us, during the past two decades or so, the concept was first extended downwards from states to individuals, upwards from the nation to the biosphere and horizontally from the military to the economic, social, political

[2] BARBARA LÜTHI (2011). Perspectives on Security in Twentieth-Century Europe and the World. Contemporary European History, 20, pp. 207-214. doi:10.1017/S0960777311000063.

and environmental[3]. While examining cyber security questions, we face a lack of definitions or non-uniform interpretation thereof, which could also be noticed at the level of presentation and disclosure of principles. It is crucial that even a threat is defined differently, therefore, different means for the reduction of the threat are employed.

5. Nature of a Strategy Document

While exploring the origin of the word "strategy", one may notice a close link thereof with the military science. Encyclopaedias indicate the origin of this concept and the connections thereof with appropriate areas of activity. The word "strategy", derived from Greek, originally meant the "art of the general", or "generalship". It has long since been broadened to include also the art of the admiral and of the air commander. So dynamic and pregnant a word is bound to be applied also to numerous other kinds of competitive situations, including commerce and games, and today one speaks of testing various "strategies of play" over a broad range of game situations[4]. A strategy: To ancient Greeks, *strategos*, from which we derive "strategy", meant simply the general's art; a modern definition, however, would generalize the meaning to a reasoned relationship among military means and the ways they might be used to reach the ends of national policy[5]. Both definitions, which have been provided, specify the military origin of the word but note that this word is also applied in many other areas of activity. There also exist very simple definitions of a "strategy", for instance, (i) a planned series of actions for achieving something; (ii) skilful planning in general[6]. The word "strategy" is very closely linked with another word originating from the military science, "tactics". "Tactics" are a means by which a strategy is carried out[7]. This means that a strategy should be achieved using "tactics"; in the case in question, separate actions and maybe even laws could be called tactical means.

According to their territorial nature, strategies may be:
- National,
- Regional,
- International and
- Global.

Currently, dominating cyber security strategies are national; the majority of the states examined have their own strategies, and for some countries, their strategy is not the first one, however, there are several regional strategies (for example, European Union) or strategies based on a certain affiliation to concrete organizations (for instance, NATO). At this point in time, there are no international or global strategies, but there exist significant initiatives, for example, The ITU National Cybersecurity Strategy Guide. If a uniform global cyber security strategy were adopted and then accepted by the majority of countries of the world, this would enable the unification of national strategies. That would be a particularly important factor influencing the solution of cyber security questions, however, there is no doubt that it will be hard to achieve that because some states arrange cyber attacks themselves for various purposes and uniform agreement will be difficult.

In order to examine the principles, it is necessary to assess which branch of social sciences these principles will belong to and what is the meaning thereof. It is important to answer the question as to what strategies are and what the purpose thereof is. This question has been analyzed quite little in the theory of social sciences. If we assessed that as "legal strategy", this concept has other meanings which are applied in choosing legal actions in order to achieve appropriate legal objectives (for instance, to win a case); in the case in question, this concept and interpretations are completely inappropriate.

[3] Rothschild, Emma. What is Security? Daedalus 124, 3 (1995), 53–98.

[4] "Strategy." International Encyclopaedia of the Social Sciences. 1968. *Encyclopedia.com.* 17 Jan. 2016. Available on the Internet: <http://www.encyclopedia.com>.

[5] John Whiteclay Chambers II. "Strategy." The Oxford Companion to American Military History. 2000. *Encyclopedia.com.* 17 Jan. 2016. Available on the Internet: <http://www.encyclopedia.com>.

[6] Longman Dictionary of Contemporary English. Available on the Internet: <http://www.ldoceonline.com/dictionary/strategy>

[7] Read more at: http://www.businessdictionary.com/definition/tactics.html#ixzz3xV8d6m3C

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online

It is vital to answer the question as to what kind of act a strategy is. Unfortunately, there are no unambiguous answers to this question, and probably there cannot be just one answer, because different states have their own specific features, i.e., for example, acts called strategies are passed departing from the means of legislating typical of legal norms or, conversely, they are passed in accordance with the procedure typical of adoption of legal acts by appropriate authorized institutions and comply with the majority of requirements for legal acts and legal norms, i.e. the formal definition and systematic character.

As mentioned above, it is important to assess what a strategy is in such a case. There is more than one definition, however, one of the short and simple definitions is the following: "A strategy is a plan for action intended to accomplish some goal"[8]. This definition m be applied in individual situations and in order to achieve more abstract objectives, therefore, the meaning of a legal strategy mentioned above may be the selection of concrete legal means in order to achieve an objective. From the systematic point of view, Cyber Security Strategies may be regarded as an action plan to achieve certain cyber security objectives; therefore, such strategies should focus on appropriate formulation of objectives and determination of how these objectives are to be achieved. In the definition of objectives and means to achieve them it is also important to formulate appropriately principles, which shoul be observed in order to achieve the objectives.

Contemporary process of legislation and democracy enables a fragmented adoption of legal norms by amending separate legal norms or parts thereof as well as adaptation of the norms to the changing social relations taking into account only separate incidents and in a very short-term perspective. Such process of legislation does not comply with the fundamental principles, i.e. predictability of law, legitimate expectations, stability of the state, etc. In order to avoid such bad practice of legislation, appropriate methodologies and means are necessary in order to improve the legislative process. How and where should the conceptual objectives and principles of the legislative process be provided?

The concept of a strategy, which originated from the military science, has been widely used in business, however, a strategy is also necessary while planning the adoption of legal norms and the activities of a state in one or another area.

Problems arise not only during the stage of development and realization of legal regulatory acts, but also during the earlier stages, i.e. while determining objectives and principles of regulatory acts to be adopted as well as the timeframe for coming into effect thereof, the funding of legal means established by legal norms, etc. The norms will be efficient only if they are in conformity with the social situation, clear objectives of legal norms are identified and there is a plan as to how the objectives will be achieved. The establishment of objectives and principles for adjustment of social relations makes it possible to forecast possible changes in norms more clearly and at the same time avoid very frequent and erroneous changes in them.

This early stage, when objectives as well as means and measures to achieve the objectives are determined, is called a strategy.

A legal strategy includes prospective planning and forecasting as well as a conceptual and long-term foresight of problems in the development of law-making.

Some strategies comply with the majority of requirements for legal norms and may be considered as legal norms with organizational elements though; however, strategies of some states may not be regarded as legal norms because they are not in conformity with all the formal attributes of a legal norm. These attributes are the following: normative nature, formal definition, universal mandatory character, guarantees of universal mandatory character (mutual benefit and a state's coercion) and systematic character. Separate strategies have a declarative, organizational nature, i.e. they do not prescribe a rule for concrete behaviour, are not universally mandatory, etc.

[8] Martha C. Nussbaum, Flawed Foundations: The Philosophical Critique of (a Particular Type of) Economics, 64 U. CHI. L. REV. 1197, 1199 (1997). 7 (defining "strategy").

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online

Considering the circumstances mentioned above, it is possible to maintain that a strategy is an organizational document which provides for measures and means to be chosen in order to achieve the objectives established in the strategy.

Taking into consideration that strategy is a high-level document it is important to find what level issues need to be developed in this document. The variety of issues discussed in existing national cybersecurity strategies are quitting big, including depth how these issues are discussed. The problem is to see all the system of state documents, therefore it is good to fix just very high level issues (like vision, goals, principles, etc.) in the strategy and to do not go more in details. Why it is important? We can divide strategies into short, medium and long-term strategies. It could be good and important discussion what particular time periods are short, medium and long for strategies in cyber security (so rapidly changing field of activities), but we need to have understanding of all of these three periods to do not lose concentration into main aims, but to stay flexible enough at the same time. Therefore, it is very important not to go into details in strategy, and to divide clearly what we can solve in the strategy, and what - in the laws.

6. Singling out Principles in Separate Strategies

The word "principle" derives from the Latin word *principium*. This word also has a number of meanings: (1) a fundamental truth or proposition that serves as the foundation for a system of belief or behaviour or for a chain of reasoning; (2) a fundamental source or basis of something[9], etc.

According to dictionaries of international words, "principle" may be described as "a conviction determining the norms of a human being's relations with the reality as well as his/her behaviour and activity". Based on the provided description, "principle" is understood in the most general sense, as a steering source substantiating the content, concrete manifestations or individual elements of a certain phenomenon. Such is, probably universally recognized, the meaning of this concept[10].

The cyber security problem encompasses many areas of human activity, and originates from a technological change, i.e. technologies enabled the emergence of the security problems under discussion. However, that is not technologies that cause problems, but people using technological possibilities, and adapting them for their purposes, i.e. the majority of problems is not of technological nature but has to do with the relation of a human being with technologies and relations of people with other people (for instance, systems are disturbed, in a targeted manner, not by technologies themselves (accidental disturbances, though, also happen due to imperfect technologies), but by people seeking selfish purposes (money, power, influence, etc.), i.e. many questions are social and they are examined by social sciences, therefore, to resolve them, the principles of social sciences are to be applied, such as the principles of law, management, economics and others.

In the examination of the principles of strategies, the main source is the texts of these strategies. Some strategies do not single out clear principles or indirectly mention isolated principles (strategies of Albania, the Netherlands, Luxembourg, Lithuania, Italy, Hungary and France), other countries single out only several clear principles in their strategies (United Kingdom (three), United States of America (three), Latvia (four), Ireland (three) and Czech Republic (three)). Some countries single out very many principles (Germany (seven), Finland (eight), Romania (eight), Estonia (eight) and Turkey (as many as thirteen)).

Some strategies clearly single out concrete principles and classify them (The strategy of Austria: "Principles related to the very strategy: comprehensiveness, integrity, proactivity and solidarity. II. Universal ICT security

[9] "principle." The Oxford Pocket Dictionary of Current English. 2009. *Encyclopedia.com*. 17 Jan. 2016. Available on the Internet: <http://www.encyclopedia.com>.

[10] "principle." The Oxford Pocket Dictionary of Current English. 2009. *Encyclopedia.com*. 17 Jan. 2016. Available on the Internet: <http://www.encyclopedia.com>.

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online

principles: confidentiality, integrity, mandatory application, authenticity, accessibility and protection of personal data. III. Fundamental principles: rule of law, subsidiarity, self-regulation and proportionality.”), in the strategies of other countries, chaos is felt and one can discuss whether what is called principles indeed are principles.

The Cyber Security Strategy of the European Union singles out five principles:
1) What applies in the physical space, also applies in the electronic space;
2) Protection of fundamental rights;
3) Access for all;
4) Management of various players;
5) Common responsibility.

When discussing these principles, it is vital to single out the most specific and important principles as well as doubtful principles. Starting with the doubtful principles, one should single out universally effective principles of general nature and principles provided for in other important documents, for example, “Protection of fundamental rights”. Does singling out of this principle, as a specific or general cyber security principle, bring something new? Would, in the absence of the Cyber Security Strategy of the European Union, this principle be ineffective or effective to a smaller extent? The content of this principle is clear enough, well-detailed in appropriate international regulatory acts and checked over and over again by authoritative international courts; and the presentation thereof in this strategy is not necessary, even though possible by showing that this is a guideline which is very important when addressing violations of this type of security, i.e. that fundamental human rights may not be sacrificed because of security solutions. Another doubtful cyber security principle is “Access for all”. This principle hardly increases security, rather reduces it, however, this principle is important from another point of view, i.e. in order to create a free and democratic community of virtual space but quite often this is what determines the vulnerability of such virtual space.

There is no doubt that the principle “What applies in the physical space, also applies in the electronic space” is a specific principle. This principle or principles very close to it are also indicated, in one way or another, in other regulatory acts regulating electronic space, for instance, the principle of non-discrimination of electronic form, etc. Another principle, which is specific indeed, as to how cyber security may be achieved is the principle of “Management of various players”, because cyber security may also be achieved using other principles, for example, the principles of centralization of appropriate resources, control or restriction, however, the concrete strategy says that cyber threats may be managed through various players.

As already mentioned, some principles could be left unmentioned, however, the presentation of all important principles in one place is valuable at least because all principles are to be applied only as part of a system, and singling out of the principles and including them into one document enable a more clear assessment of the entirety and system of principles.

NATO singles out three principles:
(1) Prevention;
(2) Resilience;
(3) Non-duplication.

This list of principles is much shorter than the lists of principles of various countries, however, these principles may be singled out as specific cyber security principles.

For a deeper analysis, a comparison may be made between the principles used by several different states.

In the 2014 strategy of Estonia, eight principles of ensuring cyber security are provided for:
1. Cyber security is an integral part of national security; it supports the functioning of the state and society, the competitiveness of the economy and innovation.
2. Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting indi-

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online

vidual liberties, personal information and identity.
3. Cyber security is ensured on the basis of the principle of proportionality while taking into account existing and potential risks and resources.
4. Cyber security is ensured in a coordinated manner through cooperation between the public-, private- and third sectors, taking into account the interconnectedness and interdependence of the existing infrastructure and services in cyberspace.
5. Cyber security starts with individual responsibility for safe use of ICT tools.
6. A top priority in ensuring cyber security is anticipating as well as preventing potential threats and responding effectively to threats that materialize.
7. Cyber security is supported by intensive and internationally competitive research and development.
8. Cyber security is ensured via international cooperation with allies and partners. Through cooperation, Estonia promotes global cyber security and enhances its own competence.

In this strategy, in addition to more general principles, which are frequent, there are also principles which are indeed interesting and important in the fight against cyber violations, for instance, how to use intensive and internationally competitive research and development for a new and rapidly-changing medium. This is a very important principle of ensuring cyber security, which is undoubtedly specific.

Some principles are also found in other strategies, for example, the principles of respect for fundamental rights, proportionality, cooperation of public and private sectors, personal responsibility and international cooperation.

In the 2014 strategy of another Baltic State, Latvia, the state principles have been formulated in a brief manner but clearly disclosed and linked to the objective: "The aim of the cyber security policy is a secure and reliable cyberspace, which ensures a safe, reliable and continuous supply of services essential for the state and society. In implementing the cyber security policy, the following principles are being used – development, cooperation, responsibility and openness." These four principles have been disclosed very thoroughly:
Development – it is possible to protect against rapidly growing threats in cyberspace only by constantly and systematically developing and improving skills in the ICT sector and its security specialisation.

Cooperation – the effective protection against threats in cyberspace unrestricted by geographical boundaries of countries or administrative boundaries of institutions is only possible through cooperation at both the national and international level.

Responsibility – it is possible to effectively reduce risks in cyberspace only if all parties involved in cyberspace, including individuals, state institutions and private businesses, are informed about and aware of the effects of their activity or inactivity on their own security and the security of others.

Openness – the cyber security policy is to be implemented by facilitating the accessibility of information and communication technology while respecting the rights and fundamental freedoms of an individual, searching for a balance between freedom, privacy and security as well as promoting good practices, ethics and standards in cyberspace.

Austria (in its 2013 strategy) singles out two important groups of principles:
"The universal Principles of ICT Security for a Digital Austria are fully applicable to cyber security: confidentiality, integrity, mandatory application, authenticity, availability as well as privacy and data protection."

The more important principles are singled out separately in the Austrian strategy and their content is explained:
"The following fundamental principles are in any case applicable to the area of cyber security:
The rule of law: Governance in the area of cyber security has to meet the high standards of the rule of law of the Austrian administration and guarantee compliance with human rights, in particular privacy and data protection, as well as the freedom of expression and the right to information.

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online

Subsidiarity: Cyber security is a legal asset. Therefore, the state pledges its strong commitment to the protection of this legal asset. However, it cannot and should not assume sole responsibility for protecting cyberspace. The owners and operators of information and communication technology (ICT) are primarily responsible for protecting their systems. The following principle shall apply: "Self-commitment if possible, regulation if necessary".

Self-regulation: Efforts should in general be made to increase the level of protection through the actors' own initiatives on the basis of code of conducts, standardisation and certification.

However, it remains the task of the state to create the regulatory framework for protecting the ICT of enterprises and private persons and to support self-regulation in the private sphere.

Proportionality: Measures to increase the level of protection and the respective costs have to be proportionate to the respective risk and to the possibilities of limiting these threats."

While analyzing the principles singled out in other strategies, one may notice that these principles are particularly different, however, the strategies mention the general principles of law and the special cyber security principles (both legal principles and other principles of social regulation). It is crucial to notice that the general principles of law are included incoherently, by singling out some of them, but not mentioning others; due to this, there remains no systematic understanding of the general principles of law, which is a faulty practice. To sum up, the enumeration of the general principles of law is possible and important, but they should be disclosed in a systematic and consistent manner; if that is not done, the enumeration thereof is not necessary and is not recommendable. It makes no sense to repeat, in the strategies, the general principles of law which are provided in Article 38 (1) (c) of the Statute of the International Court of Justice as "general principles of law recognized by civilized nations", because these principles must be effective in civilized countries as it is, therefore, it is advisable to focus on the specific principles which are characteristic only of strategies or are used in order to ensure cyber security.

The situation is completely different when it comes to the special principles. If we maintain that a strategy is a consistent universal act establishing a cyber security regulation strategy, then the identification of the special principles, and maybe even the disclosure of the content thereof, is vital. Applying the principles provided for in the strategies, it is possible to develop legal regulation more consistently as well as develop other social relations.

7. Conclusions

The principles of a democratic society make it possible to create regulation in a fragmented manner according to separate initiatives raised lawfully by interest groups, however, for the entire regulation process to be consistent, planning and the establishment of guidelines in regulation are necessary; the process of planning and forecasting is established by a strategy. A strategy may be a regulatory act possessing all the attributes of a regulatory act, however, even if a strategy does not possess certain attributes of a regulatory act, it most often is an organizational document which describes and identifies a problem to be solved as well as establishes objectives and measures and means to achieve the objectives provided for in the strategy. Such a document enables consistent planning, anticipating and forecasting of long-term trends of the development of an appropriate question, which makes it possible to provide for, in a consistent and timely manner, correctional measures of a social relation, including mandatory rules establishing legal norms, which establish and correct society's social behaviour. Strategies have an even greater meaning and value when relatively new phenomena are regulated and when there are no well-established global standards as to how emerging problems should be addressed; this makes it possible not only to appropriately regulate the relations, but also save resources. Forecasting of social relations enables the reduction in the adoption of unnecessary and untimely legal norms, which do not meet the needs, or the establishment of another regulation as well as provides the guidelines as to when it is necessary to adopt appropriate legal norms and different regulation so that one is not late with appropriate regulation of the

relations; this ensures more efficient development of comprehensive regulation.

Cyber security strategies of different states have similar structural elements of a document, for instance, objectives to be achieved which are established, principles, etc. However, the disclosure and description of these elements are quite different. The article has focused on the principles of implementation of cyber security strategies. Strategies identify different principles of social sciences (management, law, politics, economics, military science, etc.). The principles singled out in some strategies raise doubts as to whether they are indeed principles, or maybe they are only means or methods to achieve an objective. Not all strategies identify concrete principles, however, certain strategies single out even more than ten principles. This demonstrates not only the variety of different means to achieve cyber security, but also a different understanding of states as to what should be reflected in the strategies and how. It should be noted that even the EU directives promoting unification do not provide for a need to establish the Principles of Ensuring Cyber Security in national cyber security strategies. While establishing the principles in strategies, it is not necessary to repeat universally acceptable principles of separate areas, for example, law (the supremacy of human rights, etc.), because a strategy may not and does not have a purpose to abolish or amend them; they are effective under other national or international regulatory acts. It is advisable to establish only special principles of cyber security strategies or principles which acquire more importance in the cyber security context than in other areas of human activity. However, it is crucial that the general or special principles included into a strategy would indeed be key for the achievement of cyber security; then, following the identification of such principles in one document, we have a consistent system of principles because principles are applied correctly only in a uniform system, while making one or another principle absolute or attaching too much significance to it may cause damage to the entire system and distort it.

Acknowledgements

This article is part of the research 'Analysis and adaptation of EU and NATO cyber security strategies: Lithuanian cyber security model', funded by the Research Council of Lithuania (Grant No. MIP-099/2015).

References

Allabouche, K.; Diouri, O.; Gaga, A.; El Amrani El Idrissi, N. 2016. Mobile phones' social impacts on sustainable human development: case studies, Morocco and Italy, *Entrepreneurship and Sustainability Issues* 4(1): 64-73. http://dx.doi.org/10.9770/jesi.2016.4.1(6)

Albanian Cyber Security Strategy, 2014. Available on the Internet: <http://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf>

Austrian Cyber Security Strategy, 2013. Available on the Internet: <https://www.bka.gv.at/DocView.axd?CobId=50999>
BSA. 2015 EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace. Available on the Internet: <http://cybersecurity.bsa.org/index.html>

Carayannis E.G., Campbel D.F.J., Efthymiopoulos M.P. 2014. Cyber-Development, Cyber_Democracy and Cyber-Defence: Challenges, Opportunities and Implications for Theory, Policy and Practice. New York: Springer.

CCDCOE. 2014 Summit Updates Cyber Defence Policy. Insider news, 24 October. Available on the Internet: <http://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html>

Council of Europe. 2001 Convention on Cybercrime, Budapest, No. 185, 23 November. Available on the Internet: <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>

Council of Europe. Chart of signatures and ratifications of Treaty 185. Available on the Internet: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=P60tWvz9>

Cyber Security Strategy for Germany, 2011. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Germancybersecuritystrategy20111.pdf>

Cyber Security Strategy in Romania, 2011. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/StrategiaDeSecuritateCiberneticaARomaniei.pdf>

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online

Cyber Security Strategy of Belgium, 2012. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf>

Cyber Security Strategy of the Czech Republic, 2015. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf>

Cyber Security Strategy of the United Kingdom, 2011. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/UK_NCSS.pdf>

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Available on the Internet: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF>

Estonian Cyber Security Strategy, 2014. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf>

European Commission. 2001. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Network and Information Security: Proposal for a European Policy Approach, COM (2001) 298 final, 6 June. Available on the Internet: <https://ccdcoe.org/sites/default/files/documents/EU-010606-NISProposal.pdf>

European Commission. 2006 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A strategy for a Secure Information Society - Dialogue, partnership and empowerment, COM(2006) 251 final, 31 May. Available on the Internet: <http://ec.europa.eu/information_society/doc/com2006251.pdf>

European Commission. 2013 Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. February 7. Available on the Internet: <http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and>

European Commission. 2013 EU Cybersecurity plan to protect open internet and online freedom and opportunity. Press Release, 7 February. Available on the Internet: <http://europa.eu/rapid/press-release_IP-13-94_en.htm>

European Commission. 2013 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN (2013) 1 final. Brussels, February 7. Available on the Internet: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667>

European Commission. 2013 Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. COM(2013) 48 final. Brussels, February 7. Available on the Internet: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666>

European Commission. 2015 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Agenda on Security. COM(2015) 185 final, Strasbourg, 28 April. Available on the Internet: <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf>

Finland‘s Cyber Security Strategy, 2013. Available on the Internet: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf

Fuschi, D.; Tvaronavičienė, M. 2014. Sustainable development, Big Data and supervisory control: service quality in banking sector, *Journal of Security and Sustainability Issues* 3(3): 5-14. http://dx.doi.org/10.9770/jssi.2014.3.3(1)

Floridi L., Taddeo M., 2014. The Ethics of Information Warfare. Springer International Publishing Switzerland. DOI 10.1007/978-3-319-04135-3.

French National Digital Security Strategy, 2015. Available on the Internet: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf

Grubicka, J.; Matuska, E. 2015. Sustainable entrepreneurship in conditions of UN (Safety) and technological convergence, *Entrepreneurship and Sustainability Issues* 2(4): 188-197. http://dx.doi.org/10.9770/jesi.2015.2.4(2)

Hiller J.S., Russel R.S., 2013. The challenge and imperative of private sector cybersecurity: An international comparison. Computer Law & Security Review, 29 (3): 236-245. Available on the Internet: <http://dx.doi.org/10.1016/j.clsr.2013.03.003>

Ignatavičius, R.; Tvaronavičienė, M.; Piccinetti, L. 2015. Sustainable development through technology transfer networks: case of Lithuania, *Journal of Security and Sustainability Issues* 4(3): 261-267. http://dx.doi.org/10.9770/jssi.2015.4.3(6)x

International Strategy for Cyberspace, 2011. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/international_strategy_for_cyberspace_US.pdf>

Klimburg A., 2012. NATO Cybersecurity Framework Manual. NATO CCD COE Publication. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

Korauš, A.; Dobrovič, J.; Ključnikov, A.; Gombár, M. 2016. Consumer approach to bank payment card security and fraud, *Journal of Security and Sustainability Issues* 6(1): 85-102. http://dx.doi.org/10.9770/jssi.2016.6.1(6)

Kremer J. F., Muller B., 2014. Cyberspace and International Relations. Springer-Verlag Berlin Heidelberg.

Latvia's Cyber Security Strategy, 2014. Available on the Internet: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/lv-ncss

Laužikas, M.; Tindale, H.; Bilota, A.; Bielousovaitė, D. 2015. Contributions of sustainable start-up ecosystem to dynamics of start-up companies: the case of Lithuania, *Entrepreneurship and Sustainability Issues* 3(1): 8-24. http://dx.doi.org/10.9770/jesi.2015.3.1(1)

Min K.S., Chai S-W., Han M., 2015. An International Comparative Study on Cyber Security Strategy. International Journal on Security and Its Applications 9 (2): 13-20. Available on the Internet: <http://dx.doi.org/10.14257/ijsia.2015.9.2.02>

National Cyber Security Strategy, 2011, Ireland. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Luxembourg_Cyber_Security_strategy.pdf>

National Cyber Security Strategy, 2013, Hungary. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf>

National Cybersecurity Strategy for Turkey, 2013. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cybersecurity-strategy-for-turkey/at_download/file>

National Cybersecurity Strategy II, 2015, Luxembourg. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Luxembourg_Cyber_Security_strategy.pdf>

National Strategic Framework for Cyberspace Security, 2013, Italy. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/IT_NCSS.pdf>

NATO. 2011. Defending the networks: The NATO Policy on Cyber Defence. Available on the Internet: <https://ccdcoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf>

NATO. 2014. Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. Press Release, 5 September, Available on the Internet: <http://www.nato.int/cps/en/natohq/official_texts_112964.htm>

NATO. 2015. Cybersecurity. November 25, 2015. Available on the Internet: <http://www.nato.int/cps/en/natohq/topics_78170.htm>

Natowatch. 2014. NATO Moves towards a 'Cold War stand-off lite': Defence Ministers Meetings in Brussels 3-4 June 2014. Briefing Paper No.52, 12 June. Available on the Internet: <http://natowatch.org/sites/default/files/briefing_paper_no.52_-_defence_ministers_meeting_june_2014.pdf>

Pauceanu, A. M. 2016. Innovation and entrepreneurship in Sultanate of 0man – an empirical study, *Entrepreneurship and Sustainability Issues* 4(1): 83-99. http://dx.doi.org/10.9770/jesi.2016.4.1(8)

Prause, G. 2016. E-Residency: a business platform for Industry 4.0?, *Entrepreneurship and Sustainability Issues* 3(3): 216-227. http://dx.doi.org/10.9770/jesi.2016.3.3(1)

Programme for the development of electronic information security (cyber security) Lithuania, 2011. Available on the Internet: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Lithuania_Cyber_Security_Strategy.pdf

Rezk, M. A.; Ibrahim, H. H.; Tvaronavičienė, M.; Sakr, M. M.; Piccinetti, L. 2015. Measuring innovations in Egypt: case of industry, *Entrepreneurship and Sustainability Issues* 3(1): 47-55. http://dx.doi.org/10.9770/jesi.2015.3.1(4)

Samašonok, K.; Išoraitė, M.; Leškienė-Hussey, B. 2016. The internet entrepreneurship: opportunities and problems, *Entrepreneurship and Sustainability Issues* 3(4): 329-349. http://dx.doi.org/10.9770/jesi.2016.3.4(3)

Segura Serrano A. 2015. Cybersecurity: towards a global standard in the protection of critical information infrastructures. EuropeanJournal of Law and Technology 6 (3). Available on the Internet: <http://ejlt.org/article/view/396/590>

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online

Stahl W.M. 2007. The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. Georgia Journal of International and Comparative Law 40: 247-273. Available on the Internet: <http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1024&context=gjicl>

The National Cyber Security Strategy Netherland, 2013. Available on the Internet: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

Tvaronavičienė, A.; Žemaitaitienė, G.; Bilevičienė, T. 2016. Ecosystem for sustainable entrepreneurship: towards smart public procurement review procedures, *Entrepreneurship and Sustainability Issues* 4(1): 39-52. http://dx.doi.org/10.9770/jesi.2016.4.1(4)

Short biographical notes

Darius Stitilis is professor at the Mykolas Romeris University (e-mail: stitilis@mruni.eu). He obtained PhD degree in law from Mykolas Romeris university in 2002 (the topic of Phd Thesis was related to the legal responsibility in cyberspace). He is the executive manager of master study program "Cyber cesurity management" at Mykolas Romeris University. His research interests include IT law, cyber security law, privacy and personal data protection law, electronic identification law, cybercrime. He has over 40 publications primarily in the field of law and IT. Under his direction, he was involved in several scientific EU and national projects. Also, he is the co-author of two scientific monographs regarding identity theft in cyberspace: legal and electronic business issues, and e-health.

OR:
Darius Štitilis
ORCID ID: orcid.org/0000-0002-9598-0712.

Paulius Pakutinskas is associated professor at the Mykolas Romeris University (e-mail: paulius.pakutinskas@mruni.eu). He obtained PhD degree in law from Mykolas Romeris university in 2009 (the topic of Phd Thesis was related to the legal regulation of electronic communications). His research interests include IT law, intellectual property, cyber security. Also, he is the co-author of scientific monographs regarding identity theft in cyberspace: legal and electronic business issues.

OR: **Paulius Pakutinskas**
ORCID ID: orcid.org/0000-0003-2179-5298

Inga Malinauskaitė is a lecturer and PhD student at the Mykolas Romeris University (e-mail: inga.malinauskaite@mruni.eu). Her PhD topic is related to regulation and protection of data subject's rights in online social networks. Her research interests include data subject's rights, data protection in relation to IT systems, intellectual property, cyber security, online security issues.

OR: **Inga Malinauskaitė**
ORCID ID: orcid.org/0000-0001-5693-7300

Uldis Kinis. In 1981, Mr. Ķinis graduated the Faculty of Law of the University of Latvia. In 2006, Mr. Ķinis was conferred the doctoral degree in Law. Since July 2007 he was elected an associate professor of the Faculty of Law of the Riga Stradiņš University [Rīgas Stradiņa universitāte]. Uldis Kinis also is Vice-President of the Constitutional Court. He is the author of more than 30 publications mainly on problems of criminal law and information communications law.

MYKOLO ROMERIO UNIVERSITETAS

SECURITY JOURNAL
ISSN: 0955-1662 (Print) 1743-4645 (Online)
https://link.springer.com/article/10.1057/s41284-016-0083-9
17 October 2016

EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis

Darius Štitilis, Paulius Pakutinskas, Inga Malinauskaitė

Abstract

Given the global nature of cyber threats, assurance of a cyber security policy is very important not only at organization level but also at national level. Currently, cyber security as such is not independently regulated internationally; therefore the role of the EU and NATO in ensuring cyber security has become particularly significant. This article presents a study which compares the cyber security policies of the EU and NATO organizations. An analysis of how national cyber security strategies correspond with the cyber security policies and the strategic directions of these organizations has been carried out. We have also carried out a comparative study of the provision of national cyber security strategies of the EU and NATO. The study reveals that regardless of similar goals, namely assurance of cyber resilience, the selected harmonization and coordination approaches, as well as norms of national cybersecurity strategies, differ.

Keywords: cyber security strategiesregulationcomparative analysisEUNATO

References

1. 'Cybercrime and cybersecurity strategies in the Eastern Partnership region. Results of a regional workshop', Chisinau, Republic of Moldova, 12–14 November 2014, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803053d2, accessed 1 February 2016.
2. BBC News (2014) World War One: How radio crackled into life in conflict, (Charlotte Dubenskij. 18 June 2014), http://www.bbc.com/news/uk-wales-27894944, accessed 4 July 2016.
3. BSA. (2015) EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace, http://cybersecurity.bsa.org/index.html, accessed 1 February 2016.
4. Carayannis, E., Campbel, D. and Efthymiopoulos, M. (2014). *Cyber-Development, Cyber_Democracy and Cyber-Defence: Challenges, Opportunities and Implications for Theory, Policy and Practice*. New York: Springer.Google Scholar
5. CCDCOE (2014) Summit Updates Cyber Defence Policy, *Insider news*, 24 October, http://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html, accessed 1 February 2016.
6. Council of Europe (2001) 'Convention on Cybercrime, Budapest', No. 185, 23 November, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561, accessed 1 February 2016.

7. Council of Europe (2016) Chart of signatures and ratifications of Treaty 185, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=P60tWvz9, accessed 1 February 2016.
8. Cybersecurity Strategy for Norway (2012) https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Norway_Cyber_Security_StrategyNO.pdf, accessed 1 February 2016.
9. Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF, accessed 1 February 2016.
10. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF, accessed February 1, 2016.
11. Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, accessed 10 August 2016.
12. ENISA. (2014) An Evaluation Framework for National Cybersecurity Strategies. November 2014, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport, accessed 1 February 2016.
13. European Commission (2001) Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Network and Information Security: Proposal for a European Policy Approach, COM (2001) 298 final, 6 June, https://ccdcoe.org/sites/default/files/documents/EU-010606-NISProposal.pdf, 1 accessed February 2016.
14. European Commission (2006) Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A strategy for a Secure Information Society – Dialogue, partnership and empowerment, COM(2006) 251 final, 31 May, http://ec.europa.eu/information_society/doc/com2006251.pdf, accessed 1 February 2016.
15. European Commission (2013a) Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN (2013)' 1 final. Brussels, 7 February. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667, accessed 1, February 2016.
16. European Commission (2013b) 'EU Cybersecurity plan to protect open internet and online freedom and opportunity', Press Release, 7 February, http://europa.eu/rapid/press-release_IP-13-94_en.htm, Accessed 1 February 2016.
17. European Commission (2013c) Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. COM(2013) 48 final. Brussels, 7 February, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666, accessed 1 February 2016.

18. European Commission (2013d) Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, 7 February, http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and, accessed 1 February 2016.
19. European Commission (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Agenda on Security. COM (2015) 185 final, Strasbourg, 28 April, http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf, accessed 1 February 2016.
20. Floridi, L. and Taddeo, M. (2014). *The Ethics of Information Warfare*. New York: Springer International Publishing. doi:10.1007/978-3-319-04135-3.CrossRefGoogle Scholar
21. Hiller, J. and Russel, R. (2013) The challenge and imperative of private sector cybersecurity: An international comparison, *Computer Law & Security Review* 29(3): 236–245. 10.1016/j.clsr.2013.03.003, accessed 1 February 2016.
22. Klimburg, A. (2012). *NATO cybersecurity framework manual*. Tallinn: NATO CCD COE Publication, NATO Cooperative Cyber Defence Centre of Excellence.Google Scholar
23. Kremer, J. and Muller, B. (2014). *Cyberspace and International Relations*. Berlin: Springer.CrossRefGoogle Scholar
24. Lee, B. (1994) Radio Intelligence Developments during World War One and Between the Wars, California Historical Radio Society, http://antiqueradios.com/chrs/journal/intelligence.html.
25. Min, K., Chai, S.-W., and Han, M. (2015) An International Comparative Study on Cyber Security Strategy. *International Journal on Security and Its Applications* 9(2): 13–20. 10.14257/ijsia.2015.9.2.02, accessed 1 February 2016.
26. NATO (2011) Defending the networks: The NATO Policy on Cyber Defence, https://ccdcoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf, accessed 1 February 2016.
27. NATO (2014) Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. Press Release, 5 September, http://www.nato.int/cps/en/natohq/official_texts_112964.htm, accessed 1 February 2016.
28. NATO (2015) Cybersecurity, 25 November 2015, http://www.nato.int/cps/en/natohq/topics_78170.htm, accessed 1 February 2016.
29. Natowatch (2014) NATO Moves towards a 'Cold War stand-off lite': Defence Ministers Meetings in Brussels 3–4 June 2014. Briefing Paper No. 52, 12 June, http://natowatch.org/sites/default/files/briefing_paper_no.52_-_defence_ministers_meeting_june_2014.pdf, accessed 1 February 2016.
30. Segura Serrano, A. (2015) Cybersecurity: towards a global standard in the protection of critical information infrastructures. *European Journal of Law and Technology* 6(3), http://ejlt.org/article/view/396/590, accessed 1 February 2016.
31. Singh, S. (2011). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Knopf Doubleday Publishing Group. ISBN 978-0-307-78784-2.Google Scholar

32. Stahl, W. (2007) The uncharted waters of cyberspace: applying the principles of international maritime law to the problem of cybersecurity. *Georgia Journal of International and Comparative Law* 40: 247–273, http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1024&context=gjicl, accessed 1 February 2016.
33. Tropina, T.and Callanan, C. (2015). *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*. New York: Springer International Publishing.CrossRefGoogle Scholar
34. Worldatlas (2016) How Many Countries are in the World? http://www.worldatlas.com/nations.htm, accessed 1 February 2016.

MYKOLO ROMERIO UNIVERSITETAS

LIETUVOS KIBERNETINIO SAUGUMO STRATEGIJOS MODELIS

Autorių kolektyvas:
dr. Darius Štitilis
dr. Paulius Pakutinskas
dr. Marius Laurinaitis
Inga Malinauskaitė-van de Castel

Mykolo Romerio universitetas
Vilnius, 2017 m. kovo mėn.